

SANRAD V-Switch

User Manual

MIG – 002 – 02



Notice

This manual contains information that is proprietary to SANRAD. No part of this publication may be reproduced in any form whatsoever without prior written approval by SANRAD.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this manual and to the StoragePro Management System and any software components contained therein are proprietary products of SANRAD protected under international copyright law and shall be and remain solely with SANRAD.

StoragePro Management System is a registered trademark of SANRAD. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

SANRAD is continually striving to provide top-of-the-line products. If you have questions, comments or require technical assistance, you can contact SANRAD Technical Support at:

US and Americas: +1- 866-301-8155

International: +972-3-941-1890

China (EMEA, Asia, ROW): +080-0972-0074

Germany: +0-8001-812-946

The Netherlands: +-8000-220-721

TECHSUPPORT@SANRAD.COM

For general information contact SANRAD at the address below or contact your local distributor.

International Headquarters

SANRAD
32 Ha Barzel
Tel Aviv
Tel: 972-3-767-4800
Fax: 972-3-647-4104
Email: info@sanrad.com

U.S. Headquarters

SANRAD, Inc.
Tel: +1-510 521-2424
Fax: 510 521-2411
Email: zophar@sanrad.com

Limited Warranty

SANRAD warrants to the CUSTOMER that the hardware in the V-Switch to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to the CUSTOMER.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and the CUSTOMER immediately notifies SANRAD or SANRAD's local agent of such defect, SANRAD or SANRAD's local agent shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that SANRAD requests the return of equipment, each party shall pay one-way shipping costs.

SANRAD shall be released from all obligations under its warranty in the event that the V-Switch has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than SANRAD's own authorized service personnel, unless such repairs by others were made with the written consent of SANRAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties, which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall SANRAD be liable for consequential damages.

SANRAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the V-Switch, and in no event shall SANRAD's liability exceed the purchase price of the Product.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to the V-Switch and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the V-Switch are provided "as is" and without warranty of any kind. SANRAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. SANRAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above, SANRAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

SANRAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or

relating to this Agreement and the V-Switch shall not exceed the sum paid to SANRAD for the purchase of the Product. In no event shall SANRAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if SANRAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

Regulatory Information

FCC-15 User Information

The V-Switch has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the V Switch is operated in a commercial environment. The V Switch generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to the radio communications. Operation of the V Switch in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

Warning per EN 55022

The V-Switch is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Safety Notices

Read and understand the following notices before installing the V-Switch.



The power plug must be accessible at all times because it serves as the main disconnecting vehicle.



Unplug the V-Switch power cord before performing maintenance procedures.



The V-Switch contains two power supply units. To disconnect the V-Switch completely, all power supply cords must be unplugged.



Do not touch the power supplies when their power cords are connected. Line voltages are present within the power supplies when their cords are connected.



The safety cover is an integral part of this product. Do not operate the unit without the safety cover firmly in place. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.



Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) shields that might disrupt other equipment; and they direct flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.



This product relies on the building's wiring for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15a U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).



The V-Switch is intended to be grounded. Ensure that the V-Switch is connected to earth ground during normal use.



When installing the V-Switch, the ground connection must always be connected first and disconnected last.



There is a danger of explosion if the motherboard battery is replaced incorrectly. Replace the battery with the same or an equivalent type as recommended by the manufacturer. Dispose of the used battery according to the manufacturer's instructions.

User Notes

SANRAD V-Switch

User Manual

MIG – 002 – 02



Notice

This manual contains information that is proprietary to SANRAD. No part of this publication may be reproduced in any form whatsoever without prior written approval by SANRAD.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this manual and to the StoragePro Management System and any software components contained therein are proprietary products of SANRAD protected under international copyright law and shall be and remain solely with SANRAD.

StoragePro Management System is a registered trademark of SANRAD. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

SANRAD is continually striving to provide top-of-the-line products. If you have questions, comments or require technical assistance, you can contact SANRAD Technical Support at:

US and Americas: +1- 866-301-8155

International: +972-3-941-1890

China (EMEA, Asia, ROW): +080-0972-0074

Germany: +0-8001-812-946

The Netherlands: +-8000-220-721

TECHSUPPORT@SANRAD.COM

For general information contact SANRAD at the address below or contact your local distributor.

International Headquarters

SANRAD
32 Ha Barzel
Tel Aviv
Tel: 972-3-767-4800
Fax: 972-3-647-4104
Email: info@sanrad.com

U.S. Headquarters

SANRAD, Inc.
Tel: +1-510 521-2424
Fax: 510 521-2411
Email: zophar@sanrad.com

Limited Warranty

SANRAD warrants to the CUSTOMER that the hardware in the V-Switch to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to the CUSTOMER.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and the CUSTOMER immediately notifies SANRAD or SANRAD's local agent of such defect, SANRAD or SANRAD's local agent shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that SANRAD requests the return of equipment, each party shall pay one-way shipping costs.

SANRAD shall be released from all obligations under its warranty in the event that the V-Switch has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than SANRAD's own authorized service personnel, unless such repairs by others were made with the written consent of SANRAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties, which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall SANRAD be liable for consequential damages.

SANRAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the V-Switch, and in no event shall SANRAD's liability exceed the purchase price of the Product.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to the V-Switch and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the V-Switch are provided "as is" and without warranty of any kind. SANRAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. SANRAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above, SANRAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

SANRAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or

relating to this Agreement and the V-Switch shall not exceed the sum paid to SANRAD for the purchase of the Product. In no event shall SANRAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if SANRAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

Regulatory Information

FCC-15 User Information

The V-Switch has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the V Switch is operated in a commercial environment. The V Switch generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to the radio communications. Operation of the V Switch in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

Warning per EN 55022

The V-Switch is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Safety Notices

Read and understand the following notices before installing the V-Switch.



The power plug must be accessible at all times because it serves as the main disconnecting vehicle.



Unplug the V-Switch power cord before performing maintenance procedures.



The V-Switch contains two power supply units. To disconnect the V-Switch completely, all power supply cords must be unplugged.



Do not touch the power supplies when their power cords are connected. Line voltages are present within the power supplies when their cords are connected.



The safety cover is an integral part of this product. Do not operate the unit without the safety cover firmly in place. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.



Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) shields that might disrupt other equipment; and they direct flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.



This product relies on the building's wiring for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15a U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).



The V-Switch is intended to be grounded. Ensure that the V-Switch is connected to earth ground during normal use.



When installing the V-Switch, the ground connection must always be connected first and disconnected last.



There is a danger of explosion if the motherboard battery is replaced incorrectly. Replace the battery with the same or an equivalent type as recommended by the manufacturer. Dispose of the used battery according to the manufacturer's instructions.

User Notes



Table of Contents

CHAPTER 1: V-SWITCH	15
V-SWITCH OVERVIEW	16
ORDER OF OPERATIONS	17
MANUAL ORGANIZATION.....	18
CLI - COMMAND LINE INTERFACE	19
TECHNICAL ASSISTANCE	20
CHAPTER 2: INSTALLING THE V-SWITCH 2000	21
CHASSIS.....	22
Front Panel	22
Back Panel	23
System Indicator LEDs	23
SURFACE MOUNTING.....	25
RACK MOUNTING	25
STORAGE PORT CONNECTIONS.....	27
NETWORK PORT CONNECTIONS	29
CONSOLE PORT CONNECTION.....	30
POWERING UP	30
CHAPTER 3: INSTALLING THE V-SWITCH 3000	33
CHASSIS.....	34
Front Panel	34
Back Panel	34
System Indicator LEDs	35
SURFACE MOUNTING.....	36

RACK MOUNTING	36
STORAGE PORT CONNECTIONS.....	37
NETWORK PORT CONNECTIONS	39
CONSOLE PORT CONNECTION.....	40
MANAGEMENT PORT CONNECTION.....	41
LCD	42
COMPACT FLASH (CF) SLOT	42
SCALABILITY PORT	43
POWERING UP	44

CHAPTER 4: V-SWITCH CONFIGURATION..... 45

INTRODUCTION TO MANAGING THE V-SWITCH	46
CONFIGURING THE V-SWITCH 3000 MANAGEMENT PARAMETERS VIA LCD	48
CONFIGURING THE MANAGEMENT CONSOLE.....	49
INITIALIZING THE V-SWITCH.....	50
CHANGING MANAGEMENT PARAMETERS	52
Changing General Management Parameters	52
Changing the Telnet Communications Port	54
Adding an SNMP Manager	54
Adding User Login Profiles	55
CONFIGURING THE STORAGE PORTS	57
Viewing SCSI Storage Ports and Bus IDs	57
Setting a SCSI Storage Port Bus ID	57
Viewing the FC Port Information	58
Configuring an FC Storage Port	58
Viewing the V-Switch World Wide Node Name	59
CONFIGURING THE NETWORK PORTS	60
Checking the IP Configurations	61
Removing an IP Address	61
DISCOVERING ISCSI TARGETS.....	63
iSCSI Discovery Session	63
SLP	63
iSNS	63
CONFIGURING ISCSI PORTALS	64
Viewing iSCSI Portals	65
Removing iSCSI Portals	65
CONFIGURING IP ROUTING	66
Adding an IP Route	67
Setting a Default Gateway	67
Checking IP Routes	68
Viewing IP Routes	68
Removing an IP Route	68

CHAPTER 5: V-SWITCH CLUSTER CONFIGURATION 71

INTRODUCTION TO V-SWITCH CLUSTERS	72
CONFIGURING A V-SWITCH CLUSTER	75
Setting the V-Switch ID	75
Adding a Neighbor	75

Working with SCSI Storage Devices	78
Maintaining Cluster Communications	78
Enabling and Disabling Failover	79
Further V-Switch Cluster Configurations	79
Viewing V-Switch Neighbor Details	80
MANAGING A CLUSTER	81
CHAPTER 6: VOLUME CONFIGURATION	83
INTRODUCTION TO VOLUME CONFIGURATION	84
IDENTIFYING AVAILABLE STORAGE DEVICES	85
CREATING A TRANSPARENT VOLUME	88
CREATING A SUBDISK (LUN CARVING)	90
CREATING A SIMPLE VOLUME	93
CREATING A CONCATENATED VOLUME	95
CREATING A STRIPED VOLUME	97
CREATING A MIRRORED VOLUME	100
Replicating Data in a Mirrored Volume	101
CREATING A RAID 10 AND RAID 0+1	103
CHAPTER 7: VOLUME EXPOSURE & SECURITY	107
INTRODUCTION TO VOLUME EXPOSURE & SECURITY	108
iSCSI Targets	108
Identities	109
Access Rights	111
Authentication	113
Default Identity	113
CREATING AN iSCSI TARGET	115
Viewing iSCSI Targets	116
Viewing iSCSI Target Details	117
Viewing Access Rights	117
CHANGING THE DEFAULT IDENTITY	119
CREATING AN IDENTITY	120
ADDING INITIATORS TO AN IDENTITY	122
ASSIGNING IDENTITY CREDENTIALS	125
Using a RADIUS Server	128
Viewing Configured RADIUS Servers	131
CONNECTING AN IDENTITY AND TARGET	132
EXPOSING AN iSCSI TARGET AND LUN	134
Viewing LUNs	136
CHAPTER 8: ADVANCED VOLUME OPERATIONS	137
INTRODUCTION TO ADVANCED VOLUME CONFIGURATIONS	138
Data Replication: Off-line versus On-line	138
Mirror versus Snapshot	138
Actual Capacity versus Potential Capacity	138
Resizing versus Expanding	138

COPYING A VOLUME (OFF-LINE COPY)	139
SYNCHRONIZING A VOLUME	140
ADDING A CHILD TO A MIRROR (ON-LINE COPY)	141
CREATING A SNAPSHOT	144
Viewing Snapshot Volumes	149
BREAKING A MIRROR	150
RESIZING A VOLUME	153
Retracting a Volume	157
EXPANDING A VOLUME	158

CHAPTER 9: ROUTINE VOLUME MAINTENANCE 161

VOLUMES	162
Renaming a Volume	162
Removing a Volume	162
Removing all Volumes in a Hierarchy	164
Replacing a Volume	165
Synchronizing a Volume	166
TARGETS AND EXPOSURE	167
Removing an LU	167
Changing iSCSI Target Parameters	167
Removing an iSCSI Target	168
Removing a RADIUS Server	168
Removing an iSNS Server	168

CHAPTER 10: ROUTINE V-SWITCH MAINTENANCE 169

GENERAL CONFIGURATION PARAMETERS	170
TELNET PORT	171
SNMP MANAGER	173
Setting an SNMP Manager	173
Removing an SNMP Manager	173
iSNS SERVER	174
Adding an iSNS Server	174
Removing an iSNS Server	174
USER PROFILES	174
Adding a User Profile	175
Changing a User Profile	175
Removing a User Profile	175
V-SWITCH	176
Resetting a V-Switch	176
Saving (Uploading) a V-Switch Database File	176
Downloading a V-Switch Configuration File	177
NETWORK INTERFACES	177
Changing an Interface Alias	178
Adding an Interface IP Address	178
Removing an Interface IP Address	179
IP ROUTING	180
Adding an IP route	180
Removing an IP route	180

DISKS AND SUBDISKS	181
Discovering Storage Devices	181
Renaming a Storage Device	182
Removing a Storage Device	183
Renaming a Subdisk	183
Removing a Subdisk	183
CLUSTERS	184
Modifying Neighbor Parameters	184
Removing a Neighbor	184
Modifying a Cluster	185
Enabling and Disabling Failover	185
V-SWITCH 3000 POWER SUPPLY	186
UPGRADING THE V-SWITCH SOFTWARE	187
V-SWITCH 3000 COMPACT FLASH	188
SAFE MODE	190
Automatic Safe Mode	190
Exporting a Corrupted Database	192
Manual Safe Mode	192
CHAPTER 11: COMMAND LINE INTERFACE	195
V SWITCH CONFIGURATION	197
init	198
admin show	198
admin add	199
admin remove	199
admin password	199
reset	200
info	200
device set	200
device set -telnet	201
fc interface show	201
fc node show	202
fc set speed	202
interface show	202
interface details	203
interface set	203
p SCSI show	203
p SCSI set busid	204
snmp manager show	204
snmp manager add	204
snmp manager set	205
snmp manager remove	205
ip config show	206
ip config set	206
ip config remove	206
ip route add	207
ip route show	207
ip route remove	208
ip isns show	208
ip isns add	208
ip isns remove	209
neighbor add	209

neighbor set	209
neighbor show	209
neighbor details	210
neighbor remove	210
cluster show	210
cluster set	211
cluster failover enable	211
cluster failover disable	211
ft show	212
ft upload software	212
ft download	212
ft export problem	213
system boot	213
system set	213
system copy	214
system show	214
VOLUME CONFIGURATION.....	215
storage discovery	216
storage blink activate	216
storage blink abort	216
storage show	216
storage disk show	217
storage disk set	217
storage alias	217
storage details	218
storage set	218
storage remove	219
subdisk create	219
subdisk show	219
subdisk details	220
subdisk alias	220
subdisk set	221
subdisk remove	221
volume show	221
volume details	222
volume alias	223
volume hierarchy	223
volume create simple	223
volume create transparent	224
volume create mirror	224
volume create concatenated	224
volume create striped	225
volume set	225
volume remove	226
volume remove -all	226
volume replace	226
volume mirror show	227
volume mirror sync	227
volume mirror dummysync	227
volume copy create	228
volume copy show	228
volume copy abort	228
volume mirror add	229
volume mirror break	229
volume resize	229

volume retract	230
volume expand	230
volume create snapshot	230
volume snapshot show	231
volume snapshot list	231
VOLUME EXPOSURE	232
iscsi portal show	233
iscsi portal create	233
iscsi portal remove	233
iscsi target show	233
iscsi target create	234
iscsi target alias	234
iscsi target set	234
iscsi target remove	235
iscsi target authentication	235
acl show	235
acl details	236
acl add	236
acl set	237
acl rem	237
acl identity show	237
acl identity details	238
acl identity create	238
acl identity delete	238
acl identity add name	239
acl identity remove name	239
acl identity add chap	239
acl identity remove chap	240
acl identity add srp	240
acl identity remove srp	240
acl identity set	241
acl up	241
acl down	241
ip radius show	242
ip radius add	242
ip radius set	242
ip radius remove	243
volume expose –new	243
volume expose	243
lu show	244
lu details	244
lu remove	245

CHAPTER 12: SAMPLE CONFIGURATIONS..... 247

SAMPLE INTRODUCTION.....	248
INSTALLING AND USING THE V-SWITCH 3000	249
REPLACING A MIRRORED VOLUME	256
REPLICATING DATA OFF-LINE	260
CONFIGURING THE V-SWITCH WITH A SINGLE IP ROUTING PATH.....	263
CONFIGURING A CLUSTER	271

INDEX..... 285



1

V-Switch

IN THIS CHAPTER

V-SWITCH OVERVIEW

The V-Switch is a storage virtualization and management solution that allows you to pool physical storage resources and re-partition the total storage capacity into virtual volumes that best meet your storage needs.

ORDER OF OPERATIONS

The V-Switch is a high performance appliance that operates in the data-path of a storage network between the hosts and storage subsystem. It provides a single, easy-to-use connectivity and management platform for administration of small to Enterprise class storage resources.

MANUAL ORGANIZATION

CLI - COMMAND LINE INTERFACE

TECHNICAL ASSISTANCE

The V-Switch enables a network administrator to create and manage virtual storage volumes using SANRAD's Volume Manager. The Volume Manager supports the creation and combination of concatenated, striped (RAID 0) and mirrored (RAID 1) volumes.

The Volume Manager provides for secure exposure of virtual volumes to hosts using the standards-based iSCSI TCP/IP-based protocol.

V-Switch Overview

The V-Switch provides protocol bridging, routing, switching and volume management in a single platform.

Figure 1, page 17, details a standard V-Switch network topology. Two V-Switches sit in the center of the network, providing load balancing and failover ability.

Above the V-Switches are IP clouds connecting the network(s) management and host stations. The hosts can connect to the V-Switch directly or via an IP cloud. An iSCSI initiator agent in the host allows access to virtual volumes in the V Switch.

Below the V-Switches are the network storage devices, which include both *JBOD* (Just a Bunch Of Disks) and RAID subsystems. The V-Switch provides the ability to connect via both SCSI and FC protocols, including FC clouds, increasing the number of potential attached storage devices.

The V-Switch can be used in two modes:

- iSCSI bridging switch
- Storage virtualization switch

End-to-end Fibre Channel protocol networks are expensive to implement. As an iSCSI bridging switch, the V-Switch acts as a protocol bridge between storage devices on a Fibre Channel network and hosts on a standard IP network.

The V-Switch also acts as a protocol bridge between SCSI storage devices and hosts on a standard IP network.

Simple exposure of each storage device as a single LUN is an inefficient use of storage resources. As a storage virtualization switch, the V-Switch enables barrier-independent storage pooling with precise LUN carving of new virtual volumes which support mirroring and striping with managed exposure.

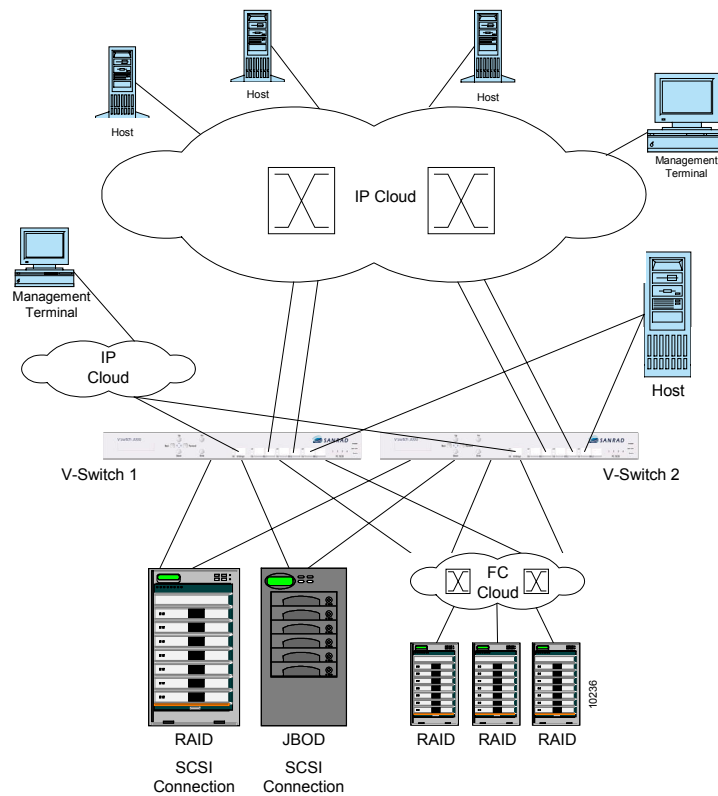


Figure 1. V-Switch Network Topology

Order of Operations

Whether being used as a bridging switch between FC or SCSI and iSCSI or as a storage virtualization switch, the V-Switch is operated in the following manner:

- STEP 1. CONNECT THE V-SWITCH TO THE REQUISITE DEVICES AND NETWORKS; POWER UP THE V SWITCH.**
- STEP 2. CONFIGURE THE V-SWITCH AND ITS INTERFACES.**
- STEP 3. CREATE VIRTUAL VOLUMES FROM THE PHYSICAL DISKS.**
- STEP 4. ASSIGN LUNS TO VIRTUAL VOLUMES; CREATE iSCSI TARGETS; ATTACH LUNS TO TARGETS AND EXPOSE TO HOSTS.**

Manual Organization

This manual is designed to guide you step-by-step through V-Switch installation, configuration, virtualization, maintenance and troubleshooting.

The chapters are set up as follows:

Table 1: Manual Chapter Organization

Chapter	Title	Description
Chapter 2	"Installing the V-Switch 2000," page 21	Explains the V-Switch2000 chassis, cabling connections and power up procedures.
Chapter 3	"Installing the V-Switch 3000," page 33	Explains the V-Switch 3000 chassis, cabling connections and power up procedures.
Chapter 4	"V-Switch Configuration," page 45	Describes how to configure the V-Switch management parameters as well as the network ports.
Chapter 5	"V-Switch Cluster Configuration," page 71	Describes how to configure V-Switches for a dual-V-Switch cluster environment.
Chapter 6	"Volume Configuration," page 83	Describes how to configure and create transparent, simple, concatenated, mirrored and striped volumes.
Chapter 7	"Volume Exposure & Security," page 107	Describes how to selectively and securely expose and manage host access to volumes.
Chapter 8	"Advanced Volume Operations," page 139	Describes how to perform on and off-line volume replication, configure snapshots and expand volumes.
Chapter 9	"Routine Volume Maintenance," page 165	Describes how to maintain and manipulate existing volumes.
Chapter 10	"Routine V-Switch Maintenance," page 173	Explains how to execute basic V-Switch maintenance functions.
Chapter 11	"Command Line Interface," page 199	Describes all CLI commands and their surrounding parameters.

Chapter	Title	Description
Appendix A	"Sample Configurations," page 251	Provides working examples of common V-Switch configurations.

CLI - Command Line Interface

The Command Line Interface (CLI) is used to implement all V-Switch management functions, including switching, virtualization and security.

The CLI is available via:

- Console port via an RS232 connection.
- 10/100 Ethernet Management port via a Telnet session (V-Switch 3000 only).
- 1 Gb Ethernet port Eth1 via a Telnet session.

All CLI commands are case sensitive and must be entered in lower case. Inputted data can include upper case letters but must always subsequently be entered in the same case.

The CLI command prompt is >.

All CLI commands in this manual are listed first with the basic command followed by a table of command switches; their explanations; status (mandatory or optional) and an example for each command switch, as shown in Table 2.

Table 2: CLI Command

`volume create transparent`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME ALIAS	USER-GIVEN ALIAS FOR THE VOLUME	OPTIONAL DEFAULT: DISK ALIAS	Transparent1
<code>-d</code>	DISK ALIAS	SYSTEM-GIVEN ALIAS FOR THE DISK DURING DISK AUTO-DISCOVERY	MANDATORY	Disk1

The CLI supports the use of the following hot keys for the listed functions:

Table 3: Hot Keys

Command	Description
?	LIST OF COMMANDS WITH A SHORT DESCRIPTION OF EACH

Command	Description
!	RETURN TO MAIN MENU
Esc	ABORT CURRENT COMMAND
#	DISPLAY LAST COMMAND TO VIEW COMMAND HISTORY
Tab	COMPLETE A COMMAND TO THE POINT OF AMBIGUITY

Technical Assistance

SANRAD is continually striving to provide top-of-the-line products. If you have questions, comments or require technical assistance, you can contact SANRAD Technical Support at:

US and Americas: 1-866-301-8155

International: +972-3-941-1890

techsupport@sanrad.com

For further information on SANRAD and the SANRAD family of products, please refer to:

<http://www.sanrad.com>

For more information on iSCSI and SCSI protocols, please refer to:

iSCSI: : <http://www.ietf.org>

iSCSI MIB: <http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-mib-03.txt>

SCSI MIB: <http://www.ietf.org/internet-drafts/draft-ietf-ips-scsi-mib-00.txt>

SCSI-3: <http://www.t10.org/scsi-3.htm>

For more information on SNMP:

SNMP: <http://www.snmpink.org/>



2

Installing the V-Switch 2000

IN THIS CHAPTER

CHASSIS

The V-Switch 2000 is a 1U high performance storage networking appliance that can be surface or rack mounted.

SURFACE MOUNTING

After mounting the V-Switch 2000, connect the requisite cables.

RACK MOUNTING

The V-Switch 2000 contains the following:

STORAGE PORT CONNECTIONS

- Two storage port connections

NETWORK PORT CONNECTIONS

- Two network port connections

CONSOLE PORT CONNECTION

- One console port connection

POWERING UP

- One onboard AC power supply

Chassis

The V-Switch 2000 is a 1 U surface or rack-mountable storage network appliance. Its front panel includes the console port, network ports, storage ports, system indicator LEDs and reset button. Its back panel includes the fans and power supply.

Front Panel

1. RS232 console port
2. Two 1 Gb copper Ethernet network port interfaces
3. Two SCSI or two FC storage port interfaces
4. Reset push button

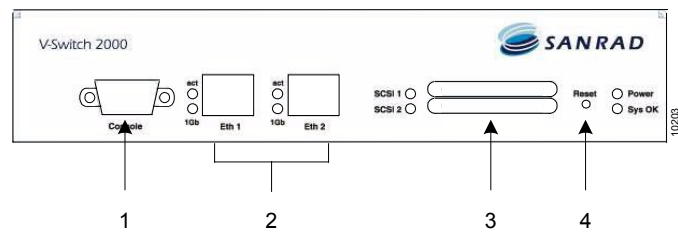


Figure 2. V-Switch 2000 Front Panel – SCSI

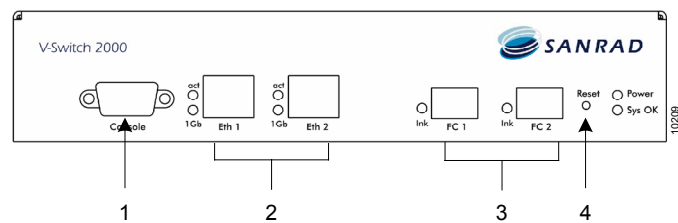


Figure 3. V-Switch 2000 Front Panel – FC

Back Panel

5. Fans
6. Power supply

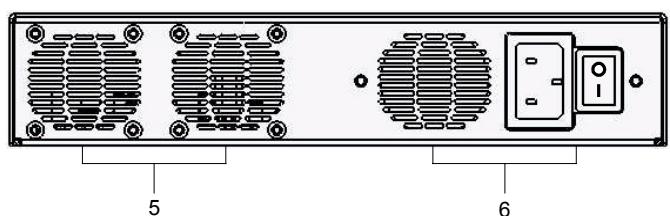


Figure 4. V-Switch 2000 Back Panel

System Indicator LEDs

Table 4 lists the V-Switch 2000 indicator LEDs as shown in Figure 5, page 24.

Table 4: V-Switch 2000 LEDs

No	LED	Status Indication	Color
1	ACT	NETWORK PORT IS ACTIVE	GREEN SLOW BLINK: ACTIVE FAST BLINK: PORT TRAFFIC
2	1GB	NETWORK PORT IS OPERATING AT 1 GB	GREEN
3	SCSI/FC	STORAGE PORT IS FUNCTIONING	GREEN
3	LNK	STORAGE PORT IS FUNCTIONING AT 1 OR 2GB	GREEN: 1 GB ORANGE: 2 GB
4	POWER	ALL POWER SUPPLIES FUNCTIONING	GREEN
5	SYS OK	ALL SYSTEMS FUNCTIONING PROPERLY	GREEN

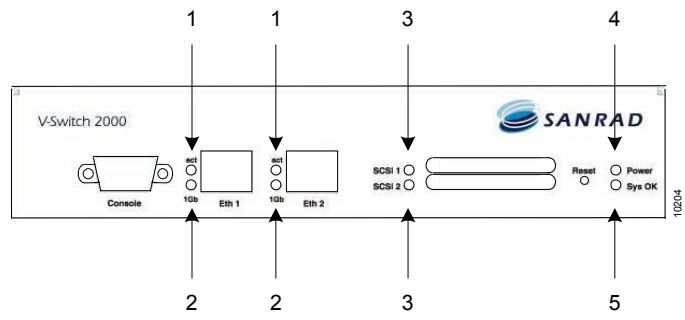


Figure 5. V-Switch 2000 LEDs – SCSI

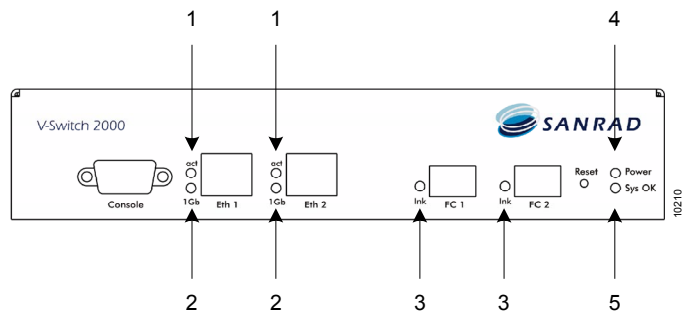


Figure 6. V-Switch 2000 LEDs – FC

Surface Mounting

The V-Switch 2000 chassis is manufactured with four chassis feet. The V-Switch 2000 is ready to be mounted on any secure flat surface. If you plan to rack mount the V-Switch 2000, continue with “Rack Mounting.”

Rack Mounting

The V-Switch 2000 chassis can be mounted on a 19-inch rack. The V-Switch 2000 can be mounted alone or two V-Switches can be joined and mounted together in a single 1U space.

The V-Switch 2000 is shipped with an accessory packet of hardware. This packet includes four non-identical L-brackets and twelve bracket screws for rack mounting

You need the following tools to rack-mount the V-Switch 2000:

- A Philips screwdriver suitable for L-bracket screws
- Four rack-post screws (and clips if necessary) suitable for the equipment rack
- A screwdriver suitable for the rack-post screws

STEP 1. PLACE THE V-SWITCH 2000 RIGHT SIDE UP ON A SECURE FLAT SURFACE NEAR THE RACK

STEP 2. ATTACH THE LEFT FRONT L-BRACKET

The left front (when facing the V-Switch) L-bracket is the wide L-bracket with two round openings for air intake.

Attach it with four of the included screws. The bracket sits directly against the V Switch.

STEP 3. ATTACH THE RIGHT FRONT L-BRACKET

There are two types of right front L-brackets, depending on if the V-Switch is single or dual-mounted.

For single-mounting, use the long arm L-bracket to span the space from the V-Switch to the rack. Attach it with four of the included screws.

For dual-mounting, use the short L-bracket on both V-Switches. Then place the two V-Switches side by side with the lip of the left V-Switch L-bracket in front of the lip of the right V-Switch L-bracket. Attach the two V-Switches by inserting two screws through the front holes of the overlapping L-brackets.

STEP 4. ATTACH THE REAR L-BRACKET

If a single V-Switch is being mounted, attach the rear L-bracket to the left side of the V-Switch.

If dual V-Switches are being mounted, attach a second rear L-bracket to the right side of the right V-Switch as well.

STEP 5. ATTACH THE V-SWITCH 2000 TO THE RACK MOUNTING POSTS

Insert the rear of the V-Switch 2000 between the rack mounting posts until the L-bracket(s) touch the rack mounting posts.

Align the mounting holes on the rear L-brackets with the mounting holes on the rack mounting posts.

Using screws that you provide, attach the V-Switch 2000 to the rack mounting posts by screwing two screws on each side through the L-brackets and into the threaded holes in the rack mounting posts.

Once the V-Switch 2000 is mounted, you can begin connecting the requisite cables.

Storage Port Connections

Connect the SAN storage devices or fabric to the V-Switch 2000 using the FC/SCSI storage ports.

The storage ports are located on the front right of the V-Switch 2000. The type of storage ports on your V-Switch 2000 will vary depending on your V-Switch 2000 order specifications – either two SCSI or two FC ports.

The V-Switch 2000 contains a storage auto-discovery function. At power-up the V-Switch 2000 automatically scans for and registers all attached and powered up network storage devices.

If you are building a V-Switch 2000 cluster, power up each disk one at a time after connecting them to the powered-up V-Switches. This allows each disk to be numbered with the same default disk number on each V-Switch 2000 during auto-discovery. This will make cluster configuration easier. For more information on V-Switch 2000 clusters, see “V-Switch Cluster Configuration,” page 71.

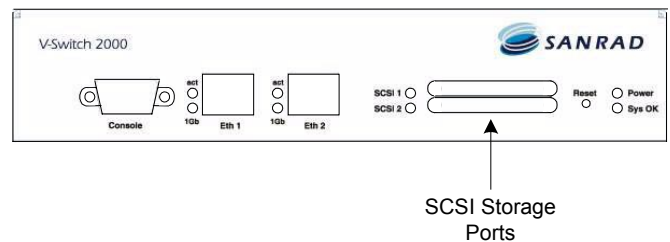


Figure 7. V-Switch 2000 SCSI Storage Ports

The V-Switch 2000 supports two storage ports in any combinations of the following:

Table 5: SCSI Storage Port Connection Type

SCSI CONNECTOR	LENGTH
SCSI ULTRA3 LVD 160MB/SEC 68 PIN PORT	UP TO 12M

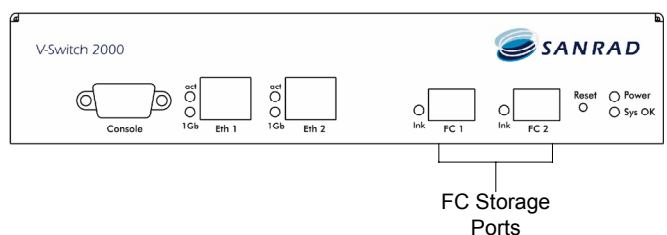


Figure 8. V-Switch 2000 FC Storage Ports

Table 6: FC Storage Port Connection Types

Your exact port configuration will depend on your V-Switch 2000 order specifications.

FIBRE CHANNEL 1 GBIT/2 GBIT NL_PORT OR N_PORT OF EITHER	LENGTH	SFP
▪ SHORT-WAVE LASER FOR MULTIMODE FIBER	UP TO 550M	SHORT-WAVE SFP
▪ LONG-WAVE LASER FOR SINGLE-MODE FIBER	UP TO 10KM	LONG-WAVE SFP
▪ COPPER (1 GBIT)	UP TO 25M	—

When connecting more than one V-Switch 2000 to a group of storage devices, ensure that the same port on each V-Switch 2000 is used to connect to the same storage device. This increases the chance of the storage device receiving the same default storage number on both V-Switches during their auto-discovery cycles. This, in turn, makes cluster configuration easier.

There are two FC storage port LEDs labeled Ink, one to the left of each storage port.

Network Port Connections

The copper network ports, labeled Eth 1 and 2, are located on the front left of the V-Switch 2000. Use the 1Gb Ethernet ports to connect to the network or directly to the host station.

When configuring your network topology, keep in mind that the current initiator technology does not support volume access by more than one server at a time. There are two methods for allowing multi-server access to a volume:

- Connect a single server to the V-Switch 2000 and allow other server to access the volume via file sharing.
- Install volume-sharing software to coordinate the read/write functionalities and data synchronization between servers.

The network ports support all of the following:

Table 7: Network Port Cable Connections

CABLE	LENGTH	SFP
1000BASE-TX (TWISTED-PAIR) OVER CATEGORY 5 UTP	UP TO 100M	—

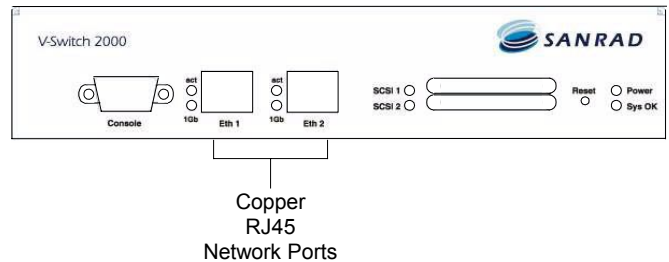


Figure 9. V-Switch 2000 Network Ports

Each network port has two LEDs:

- **act** – indicates whether the port is connected and active: slow blink – active; fast blink – port traffic.
- **1 Gb** – indicates whether the port is operating at 1 Gb. The LED is off if the port is operating at 10/100.

Console Port Connection

The console port, labeled Console, is located on the front left of the V-Switch 2000. Use this RS232 port and included male-female straight cable to connect a console or dumb terminal to the V-Switch 2000 for initial system configuration and local management.

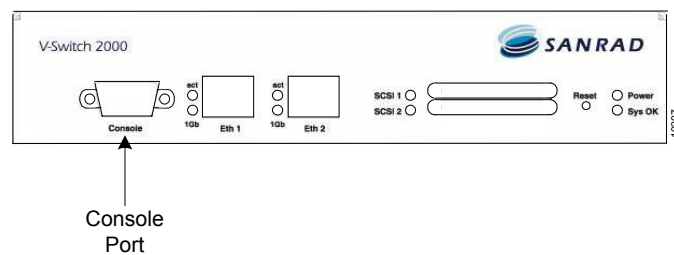


Figure 10. V-Switch 2000 Console Port

Powering Up

Do not power the V-Switch 2000 up and down quickly. The power supply is protected against electrical surges and needs at least 5 seconds between power down and power up.

You can power up the V-Switch 2000 once you have connected and powered up the storage devices. The V-Switch 2000 contains a storage auto-discovery function. At power-up the V-Switch 2000 automatically scans for and registers all attached and powered up network storage devices. Therefore, power up all storage devices **before** powering up the V-Switch 2000. Storage devices added after V-Switch 2000 power-up will be registered in the next V-Switch 2000 storage network scan.

The V-Switch 2000 contains one onboard auto-switch 100V/230V AC power supply.

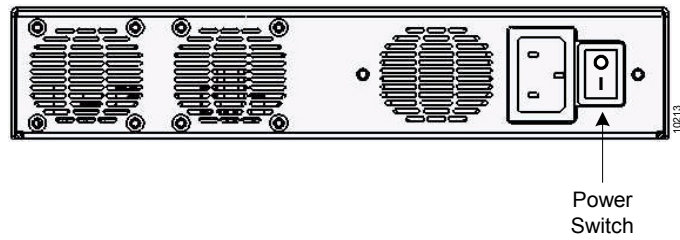


Figure 11. V-Switch 2000 Power Supplies

Reconfirm that all storage devices are powered up. Plug the power cable into the V-Switch 2000 power supply and then into the power source. Push the power switch to the ON position. The V-Switch 2000 powers up.

- The Power indicator LED on the front right of the V-Switch 2000 turns green.
- Each network port 1 Gb indicator LED turns green only if connected to the network and operating at 1 Gb.
- Each storage port indicator LED on the front right of the V-Switch 2000 is green if connected to storage.@@ One color if connected and another color if operating at the same speed.
- The fans start operating.

You are now able to initialize the V-Switch 2000.

User Notes



Installing the V-Switch 3000

IN THIS CHAPTER

CHASSIS

SURFACE MOUNTING

RACK MOUNTING

STORAGE PORT CONNECTIONS

NETWORK PORT CONNECTIONS

CONSOLE PORT CONNECTION

MANAGEMENT PORT CONNECTION

LCD

COMPACT FLASH (CF) SLOT

SCALABILITY PORT

POWERING UP

The V-Switch 3000 is a 1U high performance storage networking appliance that can be surface or rack mounted.

After mounting the V-Switch 3000, connect the requisite cables.

The V-Switch 3000 contains the following:

- ❑ Up to four storage port connections
- ❑ Three network port connections
- ❑ One management port connection
- ❑ One console port connection
- ❑ One Compact Flash (CF) slot
- ❑ One scalability port connection
- ❑ Two removable redundant AC power supplies

Chassis

The V-Switch 3000 is a 1 U surface or rack-mountable storage network appliance. Its front panel includes the LCD display and programming buttons, system indicator LEDs and network ports. Its back panel includes the storage ports, redundant power supplies, compact flash and console port.

Front Panel

1. LCD display
2. LCD display programming buttons
3. One 10/100 Management Port
4. Three 1 Gb Ethernet Network Ports; both copper and FO interfaces
5. System Indicator LEDs

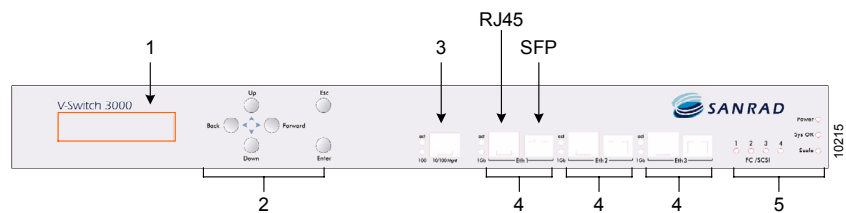


Figure 12. V-Switch 3000 Front Panel

Back Panel

6. Two - four SCSI / Fibre Channel Storage Ports
7. Dual fault tolerant power supplies
8. Removable Compact Flash (CF) slot
9. Scalability Port
10. RS232 Console Port

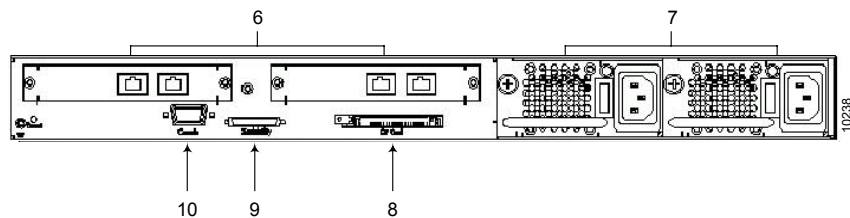


Figure 13. V-Switch 3000 Back Panel

System Indicator LEDs

Table 8 lists the V-Switch 3000 indicator LEDs as shown in Figure 14.

Table 8: V-Switch 3000 LEDs

No	LED	Status Indication	Color
1	POWER	ALL POWER SUPPLIES FUNCTIONING	GREEN
2	SYS OK	ALL SYSTEMS FUNCTIONING PROPERLY	GREEN
3	SCALE	SCALABILITY PORT IS FUNCTIONING <i>CURRENTLY NOT SUPPORTED</i>	GREEN
4	ACT	MANAGEMENT PORT IS ACTIVE	GREEN ON: ACTIVE BLINKING: PORT TRAFFIC
5	100	MANAGEMENT PORT IS OPERATING AT 100 MBPS	GREEN
6	ACT	NETWORK PORT IS ACTIVE	GREEN SLOW BLINK: ACTIVE FAST BLINK: PORT TRAFFIC
7	1GB (SCSI)	NETWORK PORT IS OPERATING AT 1 GB	GREEN: 1 GB
8	SCSI	STORAGE PORT IS FUNCTIONING	GREEN: NEGOTIATED STORAGE
8	FC	STORAGE PORT IS FUNCTIONING	GREEN: 1 GB AMBER: 2 GB*

*ONLY ON CERTAIN ALL-FC MODELS

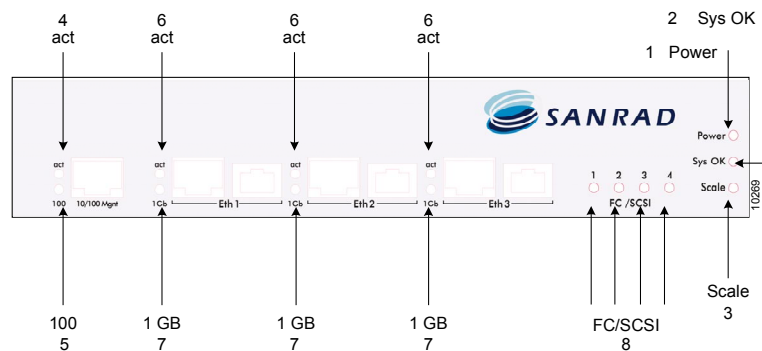


Figure 14. V-Switch 3000 LEDs

Surface Mounting

The V-Switch 3000 chassis is manufactured with four chassis feet. The V-Switch 3000 is ready to be mounted on any secure flat surface. If you plan to rack mount the V-Switch 3000, continue with “Rack Mounting.”

Rack Mounting

The V-Switch 3000 chassis can be mounted on a 19-inch rack.

The V-Switch 3000 is shipped with an accessory packet of hardware. This packet includes two L-brackets, two rear mounts (one left and one right) and ten bracket screws for mounting the L-brackets.

You need the following tools to rack-mount the V-Switch 3000:

- A Philips screwdriver suitable for L-bracket screws
- Eight rack-post screws (and clips if necessary) suitable for the equipment rack; four for the front mounts and four for the rear mounts
- A screwdriver suitable for the rack-post screws

STEP 1. ATTACH THE REAR MOUNTS

Using screws that you provide, attach the rear mounts to the back mounting posts so that the length of each mount is parallel to the floor and extends forward into the rack space.

The lip of each mount is at the bottom and facing inward toward the opposite rear mount.

The rear of the V-Switch 3000 will be supported from underneath on these lips.

STEP 2. PLACE THE V-SWITCH 3000 RIGHT SIDE UP ON A SECURE FLAT SURFACE NEAR THE RACK

STEP 3. ATTACH THE L-BRACKETS ON BOTH SIDES OF THE CHASSIS

Use the ten screws included in the accessory packet to attach the L-brackets to the chassis.

STEP 4. INSERT THE V-SWITCH 3000 INTO THE RACK

This step works best with two people.

This step works best with two people: one at the rear of the rack coordinating the V-Switch/mount connection and one at the front of the rack inserting the V-Switch.

Slide the V-Switch 3000 into the rack making sure to position the V-Switch 3000 to rest on the rear mounts.

The rear mounts may turn inward slightly before the V-switch 3000 is inserted. If the V-Switch does not enter easily, push the mount lips outward slightly while inserting the V-Switch 3000.

Insert the rear of the V-Switch 3000 until the L-brackets touch the rack mounting posts.

STEP 5. ATTACH THE V-SWITCH 3000 TO THE RACK MOUNTING POSTS

Align the mounting holes on the L-brackets with the mounting holes on the rack mounting posts making sure that the L-brackets are the same height as the rear mounts.

Using screws that you provide, attach the V-Switch to the rack mounting posts by screwing two screws on each side through the L-brackets and into the threaded holes in the rack mounting posts.

Once the V-Switch 3000 is mounted, you can begin connecting the requisite cables.

Storage Port Connections

Connect the SAN storage devices or fabric to the V-Switch 3000 using the FC/SCSI storage ports.

The storage ports are located on the back upper left of the V-Switch 3000. The number and configuration of storage ports on your V-Switch 3000 will vary depending on your V-Switch 3000 order specifications.

The V-Switch 3000 contains a storage auto-discovery function. At power-up the V-Switch 3000 automatically scans for and registers all attached and powered up network storage devices.

If you are building a V-Switch 3000 cluster, power up each disk one at a time after connecting them to the powered-up V-Switches. This allows each disk to be numbered with the same default disk number on each V-Switch 3000 during auto-discovery. This will make cluster configuration easier. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

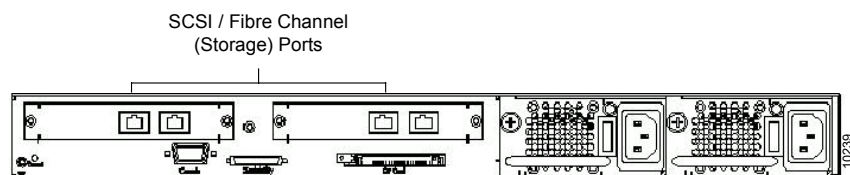


Figure 15. V-Switch 3000 Storage Ports

When connecting more than one V-Switch 3000 to a group of storage devices, ensure that the same port on each V-Switch 3000 is used to connect to the same storage device. This increases the chance of the storage device

receiving the same default storage number on both V-Switches during their auto-discovery cycles. This, in turn, makes cluster configuration easier.

The V-Switch 3000 supports up to four storage ports in any combinations in pairs of the following:

Table 9: Storage Port Connection Types

Your exact port configuration will depend on your V-Switch 3000 order specifications.

FC CONNECTOR	LENGTH
FIBRE CHANNEL 1 GBIT/2 GBIT NL_PORT OR N_PORT OF EITHER: <ul style="list-style-type: none"> ▪ SHORT-WAVE LASER FOR MULTIMODE FIBER ▪ LONG-WAVE LASER FOR SINGLE-MODE FIBER ▪ COPPER (1 GBIT) 	UP TO 550M UP TO 10KM UP TO 25M
SCSI ULTRA3 LVD 160MB/SEC 68 PIN PORT	UP TO 12M

There are four storage ports LEDs, labeled FC/SCSI 1, 2, 3 &4, on the front right of the V-Switch 3000 for up to four storage ports.



Figure 16. V-Switch 3000 Storage Port LEDs

Network Port Connections

The network ports, labeled Eth 1, 2 & 3, are located on the front right of the V-Switch 3000. Use the 1Gb Ethernet ports to connect to the network or directly to the host station.

Each network port has both a fiber optic and copper connector but only one cable, either fiber optic or copper, can be connected to each port. To connect a fiber-optic cable you need a Small Form Factor Package (SFP) optical transceiver to couple to the fiber optic cable and insert into the network SFP port. Please refer to Figure 17, page 40.

A copper connection will not work if an SFP is present in the port.

At power up, the V-Switch 3000 automatically registers which connector, copper or fiber optic, is active by searching for an SFP optical transceiver. The presence of an SFP will automatically determine which mode is active.

Once the port is active in one mode, it will not change modes unless the first, active connection is broken first. This means that once the port is active over a copper connection, the insertion of an SFP optical transceiver into the fiber optic connector will not change the port activity to fiber optic. The copper connection must first be broken and then the fiber optic connection made.

Conversely, if a port is active on a fiber optic connection and you want to switch to copper, it is not enough to remove the fiber optic connection from the SFP optical transceiver. The SFP optical transceiver must also be removed from the fiber optic connector. Only then can the port activity switch to a copper connection.

When configuring your network topology, keep in mind that the current initiator technology does not support volume access by more than one server at a time. There are two methods for allowing multi-server access to a volume:

- Connect a single server to the V-Switch 3000 and allow other servers to access the volume via file sharing.
- Install volume-sharing software to coordinate the read/write functionalities and data synchronization between servers.

The network ports support all of the following:

Table 10: Network Port Cable Connections

CABLE	LENGTH	SFP
1000BASE-SX SHORT-WAVE LASER FOR MULTIMODE FIBER	FROM 275M TO 550M	SHORT-WAVE SFP
1000BASE-LX LONG-WAVE LASER FOR SINGLE MODE FIBER	UP TO 10KM	LONG-WAVE SFP

CABLE	LENGTH	SFP
1000BASE-TX (TWISTED-PAIR) OVER CATEGORY 5 UTP	UP TO 100M	—

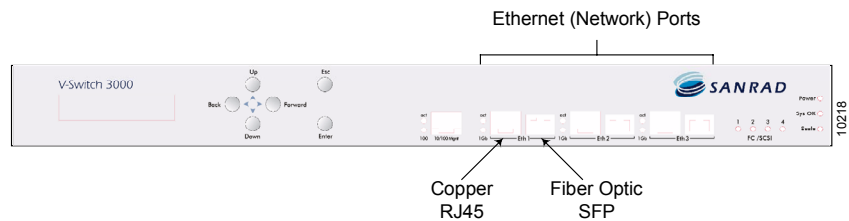


Figure 17. V-Switch 3000 Network Ports

Each network port has two LEDs:

- **act** - indicates whether the port is connected and active: slow blink - active; fast blink - port traffic.
- **1 Gb** - indicates whether the port is operating at 1 Gb. The LED is off if the port is operating at 10/100.

Console Port Connection

The console port, labeled Console, is located on the back lower left of the V-Switch 3000. Use this RS232 port and included male-female straight cable to connect a console or dumb terminal to the V-Switch 3000 for system configuration.

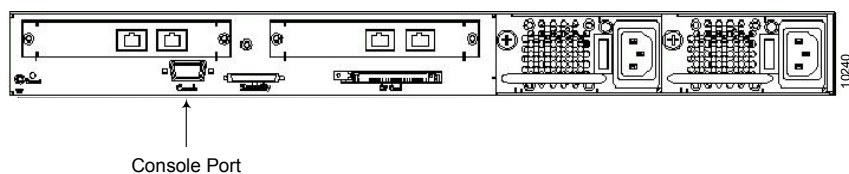


Figure 18. V-Switch 3000 Console Port

Management Port Connection

The management port, labeled 10/100 mgmt, is located on the front center of the V-Switch 3000. Use this 10/100 port to connect a host station either directly or via a network to the V-Switch 3000. When connecting directly to the V-Switch 3000 via 10/100, use a male-female straight cable. When connecting via a network, use a standard network cable. For more information on V-Switch 3000 management options, please refer to “Introduction to Managing the V-Switch,” page 46.

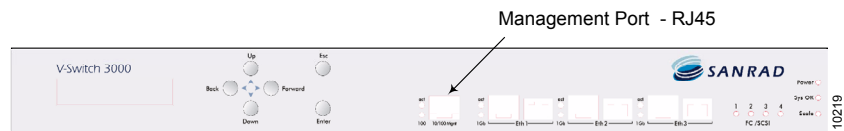


Figure 19. V-Switch 3000 Management Port

The management port has two LEDs:

- **act** – indicates whether the port is connected and active: green – active; blinking – port traffic
- **100** – indicates how the port is operational: on – 100; off – 10.

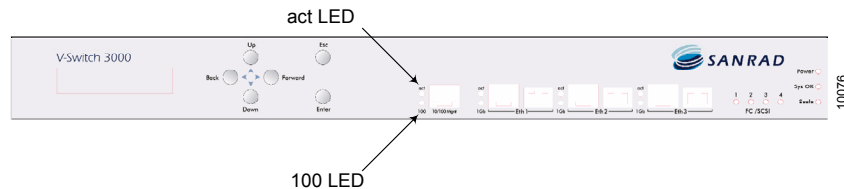


Figure 20. V-Switch 3000 Management Port LEDs

LCD

The LCD is located on the front left of the V-Switch 3000. The LCD has two rows of 16 characters each in addition to six control buttons. Use the LCD buttons and display for initial V-Switch 3000 configurations immediately after power up. For more information on configuring the V-Switch 3000 via LCD, please refer to “Configuring the V-Switch 3000 Management Parameters via LCD,” page 48.



Figure 21. LCD Display Panel

Compact Flash (CF) Slot

The compact flash slot, labeled CF Card, is located on the back center of the V-Switch 3000. A compact flash card is inserted into the slot and the configuration database is mirrored into the flash card for configuration recovery if replacing a V-Switch 3000.

Scalability Port

The scalability port is for future use and is not supported currently. The scalability port, labeled Scalability, is located on the back lower left side of the V-Switch 3000. The scalability port is a V-Switch 3000 interconnectivity port. Using SANRAD's proprietary scalability cable, two V-Switches can be connected and synchronized to function as one V-Switch 3000 to provide resource sharing and computational power increase.

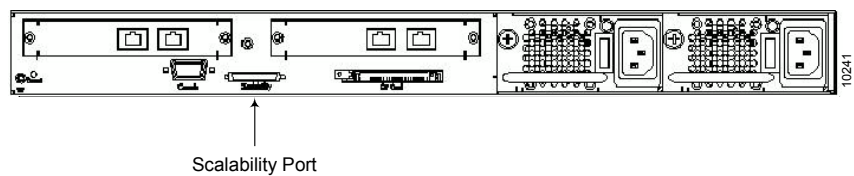


Figure 22. Scalability Port

The scalability port has one LED, labeled Scale, on the front right of the V-Switch 3000 to indicate operability.



Figure 23. Scalability Port LED

Powering Up

You can power up the V-Switch 3000 once you have connected and powered up the storage devices. The V-Switch 3000 contains a storage auto-discovery function. At power-up the V-Switch 3000 automatically scans for and registers all attached and powered up network storage devices. Therefore, power up all storage devices **before** powering up the V-Switch 3000. Storage devices added after V-Switch 3000 power-up will be registered in the next V-Switch 3000 storage network scan.

The V-Switch 3000 contains two removable auto-switch 100V/230V AC redundant power supplies.

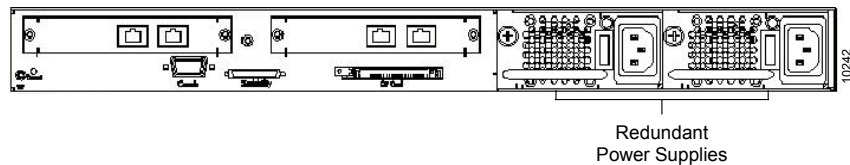


Figure 24. V-Switch 3000 Power Supplies

Reconfirm that all storage devices are powered up and connected to the V-Switch. Plug the power cables into the V-Switch 3000 power supplies and then into the power source. Push the power switch to the ON position. The V-Switch 3000 powers up.

- The Power indicator LED on the front right of the V-Switch 3000 turns green.
- Each network port 1 Gb indicator LED turns green only if connected to the network and operating at 1 Gb.
- Each storage port indicator LED on the front right of the V-Switch 3000 is green if connected to storage.
- The fans start operating.
- The LCD panel displays “V-Switch 3000 SANRAD Corp.”

You are now able to initialize the V-Switch 3000.



V-Switch Configuration

IN THIS CHAPTER

INTRODUCTION TO
MANAGING THE V-
SWITCH

CONFIGURING THE V-
SWITCH 3000
MANAGEMENT
PARAMETERS VIA LCD

CONFIGURING THE
MANAGEMENT
CONSOLE

INITIALIZING THE V-
SWITCH

CHANGING
MANAGEMENT
PARAMETERS

CONFIGURING THE
STORAGE PORTS

CONFIGURING THE
NETWORK PORTS

DISCOVERING ISCSI
TARGETS

CONFIGURING ISCSI
PORTALS

CONFIGURING IP
ROUTING

After the V-Switch is connected properly to the physical disks, management station and the network and powered up, the V-Switch must be configured.

The basic V-Switch configurations define the management IP configurations and can be done either via the LCD panel for the V-Switch 3000 or the RS232 console port for both the V-Switch 3000 and the V-Switch 2000.

Once the management port is configured, any other V-Switch configuration can be executed through the management port or continued through the RS232 console port.

Disks and LUNs connected to the storage ports are discovered and registered automatically.

Introduction to Managing the V-Switch

After powering up the V-Switch you must configure its management parameters before doing any other configuration operations, namely creating virtual disks.

This basic configuration can be done using the V-Switch LCD panel or via a console or dumb terminal to open a direct connection with the V-Switch's RS232 console port.

The V-Switch can be managed in one of three different ways with each requiring a different management configuration.

- **Out-of-band:** The management terminal connects to the V-Switch's dedicated 10/100 management port via a fast Ethernet network to pass management commands to the V-Switch in a Telnet session. This is the most secure type of management connection for the V-Switch. Please refer to A in Figure 25, page 47. The management IP address entered in the initialization command is assigned to the 10/100 management port by default for out-of-band management.
- **In-band:** The management terminal connects to the V-Switch's first 1Gb Ethernet network port, Eth1. This type of connection uses the same Ethernet network to pass management commands to the V-Switch in a Telnet session as the hosts use for accessing storage data. Please refer to B in Figure 25, page 47. You can configure the management IP address to Eth1 via the LCD or an initial out-of-band connection using the CLI command `init`. If the management port is not set to Eth1 during initialization, you will need the CLI command `device set` to set the management port to Eth1 for in-band management.
- **RS232:** The management terminal connects to the V-Switch's RS232 console port to pass management commands to the V-Switch in a direct connection. Please refer to C in Figure 25, page 47. The management IP address mandatory in the initialization command and assigned to the 10/100 management port by default for out-of-band management, will go unused in actuality.

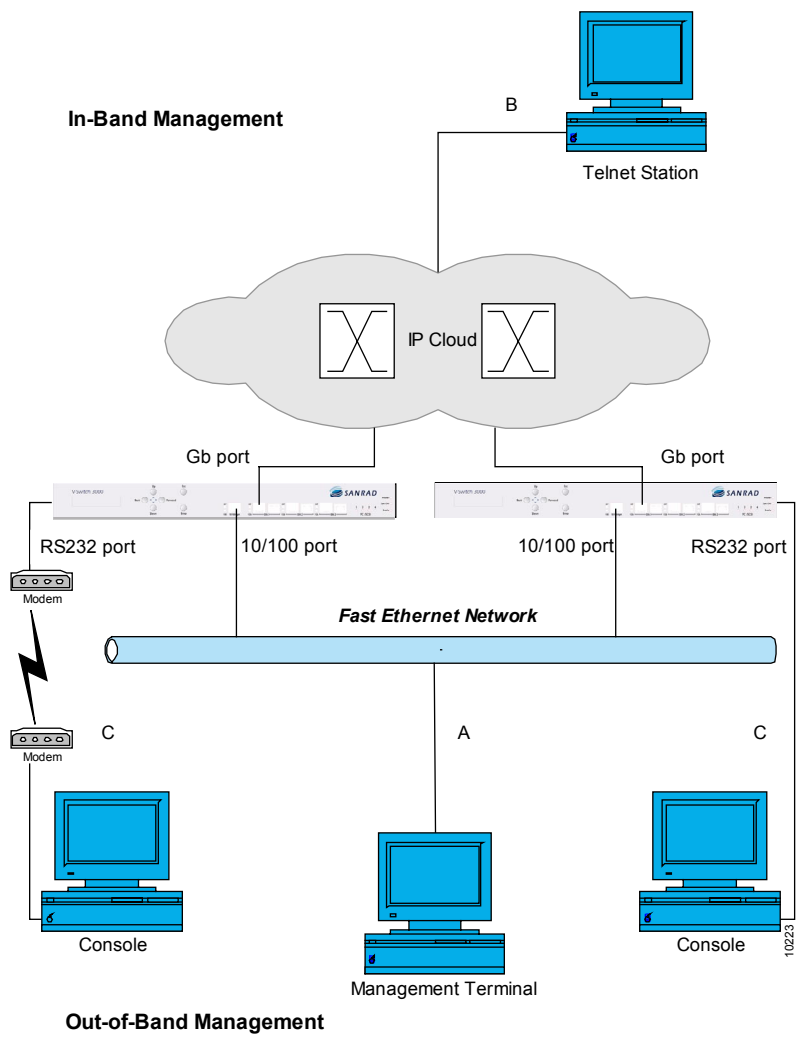


Figure 25. V-Switch Management Options

Configuring the V-Switch 3000 Management Parameters via LCD

After successfully powering up, the V-Switch 3000 LCD display panel displays:

```
V-Switch 3000
Status: OK
```

Using the Enter and arrow buttons, you toggle between LCD screens and input the V-Switch management parameters. The **Back** and **Forward** buttons toggle between spaces. The **Up** and **Down** buttons scroll between values in a space. Press **Esc** at any time to escape from a field or return to the previous screen level.

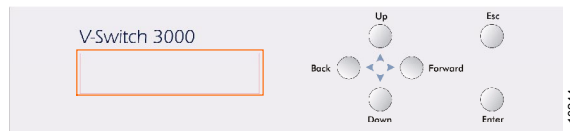


Figure 26. LCD Display Panel and Buttons

STEP 1. TOGGLE TO THE IP CONFIGURE SCREEN

The default management port via LCD is Eth1.

From the main status screen, press **Enter**. The **IP Configuration** screen appears.

```
IP CONFIG
```

Press **Enter** again. The **IP Config Eth1 Port** screen appears.

```
IP Config
ETH1 Port
```

Press **Enter** again. The **Insert IP** screen appears.

Use the Back and Forward buttons to toggle to the desired interface: mgn or eth1.

STEP 2. ENTER MANAGEMENT PORT IP ADDRESS

Enter the management port IP address using the arrow buttons. The **Back** and **Forward** buttons toggle between spaces. The **Up** and **Down** buttons scroll between values in a space.

```
Insert IP
- - - - -
2 1 2.1 9 9.0 4 3.0 4 6
```

Press **Enter** to enter the IP address and progress to the **IP Mask** screen.

STEP 3. ENTER MANAGEMENT PORT IP MASK

Enter the management port IP mask using the arrow buttons.

```
Mask
- - - - -
2 5 5.2 5 5.2 5 5.0 0 0
```

Press **Enter** to enter the IP mask and return to the main **V-Switch Status** screen.

```
V-Switch 3000
Status: OK
```

After initializing the V-Switch via the LCD display panel and buttons, you are ready to connect your management station to the V-Switch via the Eth1 management port and appropriate cable.

You are now ready to log in to the V-Switch. Continue with “Initializing the V-Switch,” page 50.

Configuring the Management Console

To configure the V-Switch management parameters via CLI, you must first open a communication session with the V-Switch via a console. From the console, you use CLI to initialize the V-Switch. Initialization includes assigning a name to the V-Switch; an IP address and mask to the management port and a UDP port for SNMP communications.

After configuring the V-Switch management parameters, you can connect a management station and log in to the V-Switch via the 1 Gb Ethernet port, Eth 1 (in-band management), the 10/100 Mb management port (out-of-band management) or continue managing the V-Switch via console.

STEP 1. CONNECT THE V-SWITCH TO A CONSOLE

Plug the included cross cable into your console’s RS232 port and then into the V-Switch’s console port, located on the back panel.

STEP 2. CONFIGURE THE CONSOLE

Configure your console according to the following parameters to communicate with the V-Switch.

PARAMETER	SYSTEM REQUIREMENT
CONFIG SERIAL PORT	COM X (ACCORDING TO YOUR PHYSICAL PORT CONNECTION)
BITS PER SECOND	115200
DATA BITS	8
PARITY	NONE
STOP BITS	1
FLOW CONTROL	NONE

After configuring the console, you can now log in to the V-Switch using your installed terminal emulation application and configure the basic V-Switch parameters. You will then be able to manage the V-Switch via the 1 Gb Ethernet port, Eth1 (in-band) or the 10/100Mb management port (out-of-band). Continue with “Initializing the V-Switch”.

Initializing the V-Switch

Before you can begin managing your storage pool, you must initialize the V-Switch. This includes assigning a name to the V-Switch; an IP address and mask for the management port and a TCP/UDP port for SNMP communications. Use the CLI command `init` to initialize the V-Switch.

If you have configured the V-Switch 3000 management IP address via LCD, you can open a Telnet session and log in to the V-Switch remotely to initialize it. If you have not configured the V-Switch 3000 management IP address or you are working with a V-Switch 2000, you can log in to the V-Switch locally via the RS232 serial connection established in the last section and initialize it.

Access to the V-Switch is password protected. The V-Switch ships with the default user name `sanrad` and the default password `sanrad`. After logging in, a total of ten user names with passwords can be configured on a V-Switch. The default user name and password `sanrad` can be maintained or removed. The user name can have from one to twenty characters. The user password can have from six to twelve characters. Both fields are case sensitive and accept all characters, including spaces.

STEP 1. OPEN A TELNET SESSION (REMOTE MANAGEMENT ONLY)

From the Windows **Start** menu, select **Run**.

In the **Open** window, enter:

```
telnet 212.199.43.46
```

Click **OK**. A Telnet session window opens.

STEP 2. LOG IN TO THE V-SWITCH

Press **Enter** on your keyboard to open the **V-Switch 3000 Login** window.

After establishing a Telnet session, you must press Enter to open the V-Switch Login window. All CLI names and aliases are case sensitive.



Figure 27. V-Switch 3000 Login Screen

Enter the default user name, **sanrad**, and password, **sanrad**, and press **Enter** on your keyboard. The CLI prompt **>** appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

STEP 3. INITIALIZE THE V-SWITCH

Use the CLI command `init` to configure the V-Switch management parameters.

`init`

You need to define five parameters to configure the V-Switch for the first time:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-n</code>	NAME	USER-ASSIGNED NAME FOR THE V-SWITCH	MANDATORY DEFAULT: VSWITCH	VSwitch
<code>-ip</code>	MANAGEMENT IP ADDRESS	IP ADDRESS OF THE MANAGEMENT PORT	MANDATORY	212.199.43.46
<code>-im</code>	MANAGEMENT IP MASK	IP MASK FOR THE MANAGEMENT PORT	OPTIONAL DEFAULT: 255.255.255.0	
<code>-p</code>	UDP PORT	PORT THROUGH WHICH ALL UDP COMMUNICATIONS WILL FLOW – NAMELY FOR SNMP	OPTIONAL DEFAULT: 161	
<code>-if</code>	INTERFACE ALIAS	ALIAS OF PORT FOR MANAGING V-SWITCH	OPTIONAL DEFAULT: MGMT (ETH1 OR MGMT)	

Example:

`init -n VSwitch -ip 212.199.43.46`

After the V-Switch is initialized, this CLI command will disappear from the CLI menu.

Changing Management Parameters

After logging in to the V-Switch, you can change the general management parameters and Telnet communications port as well as add user login profiles.

Changing General Management Parameters

You can change V-Switch management parameters (IP address and mask) or UDP port number as well as include details of whom to contact in the event of technical difficulties and which read/write communities to send traps to. Use the CLI command **device set** to add or change management parameters. This command will not appear in the CLI menu until the V-Switch is initialized.

device set

You can define or change thirteen parameters using this command:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-n	NAME	USER-ASSIGNED NAME FOR THE V-SWITCH	OPTIONAL	VSwitch1
-ip	MANAGEMENT IP ADDRESS	IP ADDRESS OF THE MANAGEMENT PORT	OPTIONAL	212.199.43.47
-im	MANAGEMENT IP MASK	IP MASK FOR THE MANAGEMENT PORT	OPTIONAL DEFAULT: 255.255.255.0	
-p	UDP PORT	PORT THROUGH WHICH ALL UDP COMMUNICATIONS WILL FLOW – NAMELY FOR SNMP	OPTIONAL DEFAULT: 161	
-if	INTERFACE ALIAS	ALIAS OF PORT FOR MANAGING V-SWITCH	OPTIONAL DEFAULT: MGMT (ETH1 OR MGMT)	
-d	DATE	LOCAL DATE	OPTIONAL	21/07/2002
-t	TIME	LOCAL TIME	OPTIONAL	13:30
-c	CONTACT	CONTACT PERSON IN THE EVENT OF A SYSTEM MALFUNCTION	OPTIONAL	AnnaLevin

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-loc	LOCATION	LOCATION OF THE CONTACT PERSON	OPTIONAL	ext4838
-rld	REPORT LUN DISCOVERY	MODE FOR DISCOVERING DEVICE LUNS	OPTIONAL YES OR NO DEFAULT: YES	no
-telnet	TELNET PORT	PORT FOR V-SWITCH COMMUNICATIONS	OPTIONAL DEFAULT: 23	1597
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	

Example:

The V-Switch alias is reset to V-Switch 1; the IP address for V-Switch management functions is changed to 212.199.43.47. The date is set to the 21st of July, 2002 and the time to 1:30 p.m. Anna Levin is named as the contact person and she can be reached at the internal office extension 4838.

```
device set -n VSwitch1 -ip 212.199.43.47 -d 21/07/2002 -
t 13:30 -c AnnaLevin -loc ext4838
```

You can now connect to the V-Switch 1 Gb Ethernet port or 10/100Mb management port and begin managing the V-Switch operations and the attached SAN.

Checking the V-Switch Configurations

After setting the general V-Switch Management configurations, you can use the CLI command **info** to access the V-Switch Configuration table and view the current configuration, including whom to contact in the event of technical difficulties.

```
info
```

Table 11: V-Switch Configuration

Parameter	Value
Name	VSwitch1
Description	SW Version 2.0, build 4,patch 0 Board version 1, PCB version 0
ID	-1
Contact	Anna Levin
Location	Ext. 4838
Status	OK

Parameter	Value
Object ID	1.3.6.1.4.1 10059 1.1.2
Time Since Last Reset	12 days 17 hours 29 min 32 sec
Mgmt IP Address	212.199.43.47
Mgmt UDP Port	161
Date & Time [DD/MM/YY]	21/04/02 13:33
Telnet Port	23
Eth	Up
FC	Up
Read Community	Public
Write Community	Private

Changing the Telnet Communications Port

If your Telnet communications connection to the V-Switch traverses a firewall, the standard Telnet communications port 23 may be blocked by the firewall as a security measure. To enable Telnet communications to the V-Switch, you can designate an alternate port using the CLI command **device set -telnet**. This port can be opened in the firewall for dedicated Telnet-V-Switch communications.

```
device set -telnet
```

Example:

The port 1597 is programmed as the Telnet communications port.

```
device set -telnet 1597
```

Use the CLI command **info** to check the V-Switch's designated Telnet port.

Adding an SNMP Manager

You can add a manager to the V-Switch. If you are working with StoragePro, the V-Switch GUI management system, StoragePro will automatically be included as a manager. If you are still not working with StoragePro, there are no default managers defined for the V-Switch. You can use the CLI command **snmp manager add** to add managers to the V-Switch.

```
snmp manager add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UPD PORT	PORT TO RECEIVE TRAPS THROUGH	OPTIONAL DEFAULT: 162	162

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	public
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	private
-trap	TRAP	TO SEND TRAPS TO MANAGER	OPTIONAL YES: SEND NO: DO NOT SEND DEFAULT: YES	yes

Example

An SNMP manager is added on IP address 212.199.43.96. It receives traps through port 162. The manager receives information through the public community and writes information through the private community.

```
snmp manager add -ip 212.199.43.96 -p 162 -rcom public -wcom private -trap yes
```

Adding User Login Profiles

All CLI names and aliases are case sensitive.

After logging in to a V-Switch, a total of ten user profiles (name plus password) can be configured on a V-Switch using the CLI command **admin add**. The default user name and password **sanrad** can be maintained or removed. The user name can have from one to twenty characters. The user password can have from six to twelve characters. Both fields are case sensitive and accept all characters, including spaces.

Example

```
admin add
```

You need to define two parameters to configure a user profile:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-un	USER NAME	USER NAME	MANDATORY	Joe Cool
-pw	PASSWORD	USER PASSWORD	MANDATORY 6 CHARACTER MINIMUM	123456

Example

```
admin add -un Joe Cool -pw 123456
```

For information on changing or removing user profiles, please see “User Profiles,” page 178.

Configuring the Storage Ports

If your V-Switch configuration contains SCSI devices, you can set the storage port bus ID. If your V-Switch configuration contains FC storage ports, you can change the default configuration of each port. Use the CLI command `interface show` to show all storage port connections.

Table 12: V Switch Interfaces

Type	Name	Description	Alias	Phys Address
RS232	cons	RS232 Management Int	cons	000000000000
ETHERNET	mgmt	Fast Ethernet Manage	mgmt	000000000000
FibreChannel	fc1	FC MMF	fc1	000000000000
FibreChannel	fc2	FC MMF	fc2	000000000000
SCSI	SCSI1	SCSI Ultra 3	SCSI1	000000000000
SCSI	SCSI2	SCSI Ultra 3	SCSI2	000000000000
ETHERNET	eth1	Gigabit Ethernet Net	eth1	00081a000110
ETHERNET	eth2	Gigabit Ethernet Net	eth2	00081a000111
ETHERNET	eth3	Gigabit Ethernet Net	eth3	00081a000112

Viewing SCSI Storage Ports and Bus IDs

Use the CLI command `p SCSI show` to view all SCSI storage ports and their corresponding SCSI bus ID.

```
p SCSI show
```

Alias	BusID
p SCSI3	12
p SCSI4	7

Setting a SCSI Storage Port Bus ID

Each storage port connected to a SCSI device must have a SCSI bus ID. Use the CLI command `p SCSI set busid` to set a storage port's SCSI bus ID.

```
p SCSI set busid
```

You need to define two parameters to set a storage port SCSI bus ID:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE	STORAGE PORT NUMBER	MANDATORY	p SCSI3
-id	IDENTITY	SCSI BUS IDENTITY	OPTIONAL DEFAULT: 7	12

Example

Storage port 3, p SCSI3, is assigned SCSI bus ID 12.

```
p SCSI set busid -if p SCSI3 -id 12
```

Viewing the FC Port Information

Use the CLI command **fc interface show** to view all FC ports on the V-Switch; their World Wide Port Names (WWPN) and administrative and operative types.

```
fc interface show
```

Alias	WWPN	Connect Mode	Oper Type	Speed
fc1	20:00:00:20:38:11:34:78	Private	NlPort	1Gbs
fc2	20:00:00:20:38:00:10:64	Private	nlPort	1Gbs

Configuring an FC Storage Port

The V-Switch default configuration for FC connections is 1 GB nl port in a public loop. If you want to change the default configuration, each storage port connected to an FC device can be reconfigured to change the connection speed, port type and connection mode. Use the CLI command **fc set** to change the FC storage port communication speed; the port type or connection mode.

```
fc set
```

You need to define four parameters to reconfigure an FC port:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE	STORAGE PORT	MANDATORY	fc2
-sp	SPEED	FC COMMUNICATION SPEED	OPTIONAL AUTO: 0 1 GB: 1 2 GB: 2	1
-pt	PORT TYPE	TYPE OF FC PORT	OPTIONAL N OR NL	nl

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-cm	CONNECTION MODE		OPTIONAL FAB: FABRIC PRL: PRIVATE LOOP PUL: PUBLIC LOOP	private

Example

```
fc set -if fc2 -sp 1 -pt nl -cm prl
```

Viewing the V-Switch World Wide Node Name

Use the CLI command `fc node show` to view the V-Switch World Wide Node Name (WWNN).

```
fc node show
```

Name	V-Switch1
Description	SW Version 1.5, build 5,patch 0 Board version 1, PCB version
WWNN	20:00:20:10:58:00:10:46
Function	Gateway

Configuring the Network Ports

Each network port must be located on a separate subnet.

Each network port can have more than one IP address.

To connect the V-Switch to the network you need to assign IP parameters to each 1Gb Ethernet network port connected to a network. Each network port must be located on a separate subnet. Each network port can have more than one IP address. Use the CLI command `ip config set` to assign IP parameters. Once configured, each network port will provide an access point for hosts to the storage network. Once access is gained, a host will be able to read from and/or write into the storage network.

`ip config set`

You need to define three parameters to configure each network port:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
	<code>-ip</code>	IP ADDRESS	IP ADDRESS ASSIGNING TO THE INTERFACE PORT	MANDATORY 212.199.43.56
	<code>-if</code>	INTERFACE ALIAS OR NAME	NETWORK INTERFACE PORT	MANDATORY ETH1, ETH2, ETH3 eth1
	<code>-im</code>	IP MASK	IP NET MASK	OPTIONAL DEFAULT: 255.255.255.0
	<code>-act</code>	ACTIVITY	IF IP ADDRESS IS ACTIVE TO EXPOSE VOLUMES. USE INACTIVE STATUS TO ALLOW FAILOVER.	OPTIONAL DEFAULT: 1 (ACTIVE) 2 (INACTIVE) 1

Executing this command on the same network port with a different IP address will not reset the network port address. It will add another IP address to the network port

For regular port activity, use the default active port setting. The inactive port setting is used when configuring a V-Switch cluster. If you are configuring a V-Switch cluster, each IP address must be configured on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

Example:

The IP address 212.199.43.56 is assigned to the 1 Gb Ethernet port Eth1.

```
ip config set -ip 212.199.43.56 -if eth1 -act 1
```

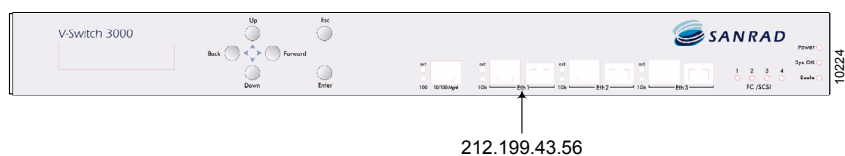


Figure 28. Ethernet Port 1 IP Address

Checking the IP Configurations

After setting the management and network port IP addresses, you can use the CLI command `ip config show` to access the IP Configuration Table and view all assigned port IP addresses.

```
ip config show
```

Table 13: V-Switch IP Configuration Table

If Name	IP Address	Net Mask	Activity
mgmt	212.199.43.46	255.255.255.0	Active
eth1	212.199.43.56	255.255.255.0	Active
eth1	212.199.43.57	255.255.255.0	Inactive
eth2	212.199.75.66	255.255.255.0	Active
eth3	212.199.12.67	255.255.255.0	Inactive
eth3	212.199.12.70	255.255.255.0	Active

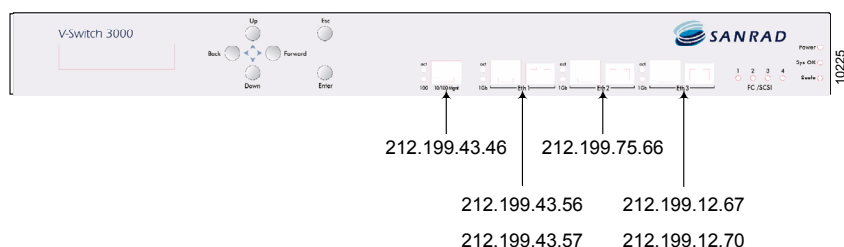


Figure 29. V-Switch IP Addresses

Removing an IP Address

An IP address that has a portal configured on it cannot be removed.

Network ports can have multiple IP addresses. You can remove an IP address that is no longer relevant from a network port using the CLI command `ip config remove`. You can remove the last network IP address from a port, but you cannot remove the management IP address from Eth1. If you are working in a cluster, the IP address must be removed from both V-Switch databases. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

`ip config remove`

You need to define one parameter to remove a network port IP address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS TO REMOVE FROM THE NETWORK INTERFACE PORT	MANDATORY	212.199.12.70

Example:

The IP address 212.199.12.70 is removed from Eth3 leaving the port with only one IP address, 212.199.12.67.

`ip config remove -ip 212.199.12.70`

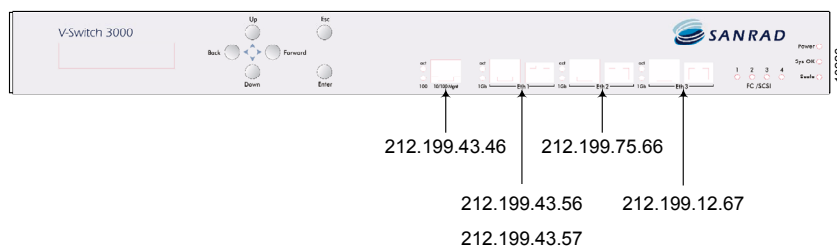


Figure 30. Ethernet Port 3 with One IP Address

Discovering iSCSI Targets

iSCSI target discovery is performed across the IP-SAN by the iSCSI initiator located on the server. The V-Switch supports three methods for reporting iSCSI targets in the IP-SAN to iSCSI initiators:

- iSCSI Discovery Session
- SLP
- iSNS

iSCSI Discovery Session

The V-Switch supports iSCSI discovery sessions for reporting iSCSI targets to iSCSI initiators. A V-Switch network IP address must be configured on the iSCSI initiator for the initiator to connect to and discover the V-Switch's attached iSCSI targets.

SLP

The V-Switch supports Service Location Protocol (SLP) by acting as an SLP Service Agent (SA). No configuration is necessary. An SLP SA services User Agents (UAs). UAs are iSCSI initiators that query a network for all attached iSCSI targets. The V-Switch supports the specific service **service:iscsi:target**.

iSNS

The V-Switch supports Internet Storage Name Service (iSNS) protocol for advertising its targets and portals on the iSNS server to enable iSCSI initiators in the IP-SAN to locate the V-Switch targets automatically. Use the CLI command **ip isns add** to add an iSCSI server to the V-Switch's iSNS client. Targets defined by the V-Switch's Access Control List (ACL) as having controlled access are accessible only to those servers defined as having access to the target. See "Volume Exposure & Security," page 107.

ip isns add

You need to define one parameter to add an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1

Use the CLI command **ip isns show** to view all added iSCSI server addresses.

```
ip isns show
```

Table 14: iSNS Servers

```
212.199.56.45
```

Deleting an iSNS Server

Use the CLI command `ip isns remove` to remove an iSNS server from the V-Switch iSNS client.

```
ip isns remove
```

You need to define one parameter to remove an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1

Configuring iSCSI Portals

Do not create an iSCSI portal on the management IP address.

The V-Switch supports a maximum of 100 portals.

To enable communication between iSCSI initiators and iSCSI targets you need to assign a portal to the iSCSI protocol transport. Use the CLI command `iscsi portal create` to create an iSCSI portal. A portal is the coupling of an IP address and a TCP port. Once created, a portal is opened automatically during a communication session. If you are working in a V-Switch cluster, each portal must be created on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

```
iscsi portal create
```

You need to define two parameters to configure an iSCSI portal:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	USER-ASSIGNED NETWORK PORT IP ADDRESS	MANDATORY	212.199.43.66
-p	TCP PORT	TCP PORT THROUGH WHICH THE iSCSI PROTOCOL PASSES	OPTIONAL DEFAULT: 3260	

Example:

An iSCSI portal is created using the default TCP port 3260 for the IP address 212.199.43.66.

```
iscsi portal create -ip 212.199.43.66
```

Viewing iSCSI Portals

You can view all created portals using the CLI command `iscsi portal show`.

```
iscsi portal show
```

Table 15: iSCSI Portals

Protocol	Address Type	Address	Port
6	ipv 4	212.199.43.56	3260
6	ipv 4	212.199.43.57	3260
6	ipv 4	212.199.43.66	5003
6	ipv 4	212.199.43.67	5003

Protocol 6 is the transport protocol for iSCSI. Address type IPv 4 designates a four byte IP address.

Removing iSCSI Portals

You can remove an iSCSI portal using the CLI command `iscsi portal remove`. Only after all iSCSI portals related to an IP address are removed from a port can the IP address be removed from the port. If you are working in a cluster, the portal must be removed from both V-Switch databases. For more information on V-Switch clusters, see “Introduction to V-Switch Clusters,” page 72.

```
iscsi portal remove
```

You need to define two parameters to remove an iSCSI portal:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF NETWORK PORT	MANDATORY	212.199.43.67
-p	TCP PORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL DEFAULT: 3260	5003

Configuring IP Routing

To enable communications between the V-Switch and IP networks located outside the V-Switch LAN, you must configure IP routing paths for each external network port. The IP route begins with a specified network port on the V-Switch and ends at the external network IP address. Just as each IP address is unique, each IP routing path is unique. There can be only one IP route to a given external network IP address per V-Switch.

In Figure 31, page 68, you have two V-Switches connected to three different LANs (A, B, C). In turn, each LAN is connected to at least one external network (D, E, F).

On V-Switch 1, network ports Eth1 and Eth2 can both access Network D:

You can configure only one IP route to a given external network on your V-Switch.

PORT	LAN	ROUTER LEG
ETH1	A	20.20.10.20
ETH2	B	30.30.20.20

Only one of these paths can be configured for V-Switch 1.

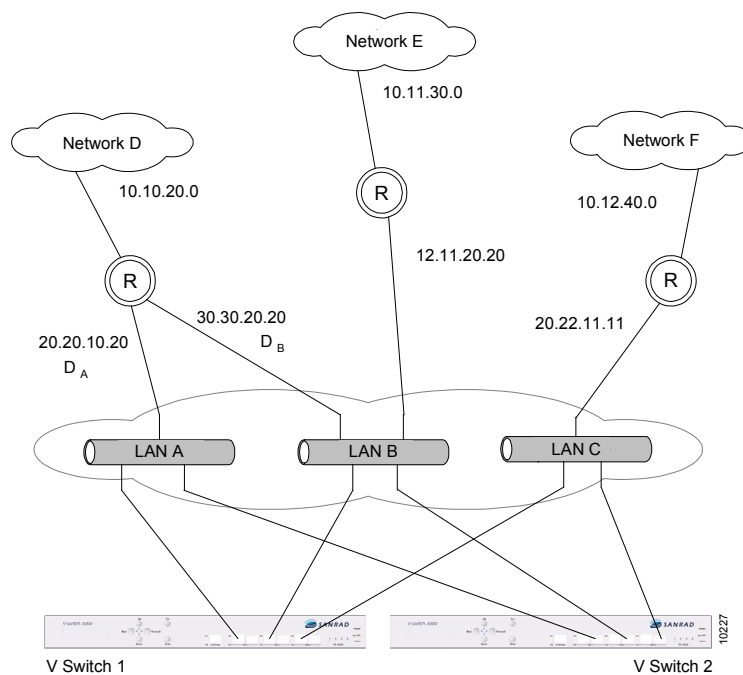


Figure 31. IP Routing Options

Adding an IP Route

You can enable communications to networks outside of your LAN by configuring an IP routing path. This allows volume access to hosts located on external networks. Use the CLI command `ip route add` to add an IP routing path to your V-Switch. If you are working in a V-Switch cluster, you must configure the IP route on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

```
ip route add
```

You need four parameters to configure an IP routing path.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-dip</code>	DESTINATION IP	IP OF HOST NETWORK	MANDATORY	<code>10.10.20.0</code>
<code>-dmask</code>	DESTINATION MASK	IP MASK OF HOST NETWORK	MANDATORY	<code>255.255.255.0</code>
<code>-gw</code>	GATEWAY IP ADDRESS	IP ADDRESS OF THE GATEWAY ROUTER	MANDATORY	<code>30.30.20.20</code>
<code>-if</code>	INTERFACE ALIAS	NETWORK PORT TO OPEN COMMUNICATION THROUGH	MANDATORY	<code>eth2</code>

Example:

An IP routing path to Network D, IP 10.10.20.0, (IP mask 255.255.255.0) is mapped from network port Eth2 through router gateway 30.30.20.20.

```
ip route add -dip 10.10.20.0 -dmask 255.255.255.0 -gw 30.30.20.20 -if eth2
```

Setting a Default Gateway

You can set a default gateway for Eth1 for working with your local gateway. This gateway is used for any IP address not specified in the V-Switch routing table. Use the CLI command `ip route default` to set the default gateway IP address for Eth1. To change the default gateway, repeat the command with the new default gateway IP address.

```
ip route default
```

You need one parameter to configure a default IP routing path.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-gw</code>	GATEWAY	IP ADDRESS OF DEFAULT GATEWAY	MANDATORY	<code>20.20.10.20</code>

```
ip route default -gw 20.20.10.20
```

Checking IP Routes

After creating an IP routing path, you can ping any IP-connected device from the V-Switch Eht1 to check that the routing is configured correctly. Use the CLI command **ping** to ping an IP address from the V-Switch. Make sure that the route is defined on the other side as well.

```
ping
```

You need one parameter to check an IP routing path from the V-Switch.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS TO PING	MANDATORY	172.17.200.69

```
ping -ip 172.17.200.69
```

Viewing IP Routes

After creating an IP routing path to an external network, you can view it and any other configured IP routing path. Use the CLI command **ip route show** to view a V-Switch's routing table.

```
ip route show
```

Table 16: V-Switch IP Routing Paths

Dest IP Address	Dest Mask	Interface	Gateway	TOS
10.10.20.20	255.255.255.0	Eth2	30.30.20.20	
10.12.40.40	255.255.255.0	Eth3	20.22.11.11	

Removing an IP Route

You can remove unwanted IP routing paths from your V-Switch. Use the CLI command **ip route remove** to remove an IP routing path. If you are working in a V-Switch cluster, the IP route must be removed from both V-Switch databases. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

```
ip route remove
```

You need three parameters to remove an IP routing path.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-dip	DESTINATION IP	IP OF HOST STATION	MANDATORY	10.12.40.0
-dmask	DESTINATION MASK	IP MASK OF HOST STATION	MANDATORY	255.255.255.0
-if	INTERFACE ALIAS	NETWORK PORT TO OPEN COMMUNICATION THROUGH	MANDATORY	eth3

Example:

The routing path to destination network IP 10.12.40.0 (IP mask 255.255.255.0) is removed from network port Eth3.

```
ip route remove -dip 10.12.40.0 -dmask 255.255.255.0 -if eth3
```

You have now configured all basic V-Switch parameters. If you are creating a V-Switch cluster, continue with “Configuring a Cluster,” page 276. If you are still working with a single V-Switch, you can now begin creating virtual volumes. Continue with “Volume Configuration,” page 83.

User Notes



5

V-Switch Cluster Configuration

IN THIS CHAPTER

INTRODUCTION TO V-
SWITCH CLUSTERS

CONFIGURING A V-
SWITCH CLUSTER

MANAGING A CLUSTER

You can configure a V-Switch cluster using two V-Switches of the same type. A *cluster* is a group of storage units and switches that function as one unit for virtualization and provide high availability in the event of V-Switch failover.

A cluster can be configured between two V-Switches using CLI or SANRAD's StoragePro management GUI. We recommend using StoragePro for its simplicity of use, particularly for cluster configuration. For more information on configuring a cluster using StoragePro, consult the StoragePro User Manual and on-line help system. If you prefer to use CLI, continue with this chapter.

If your network still contains only one V-Switch, you can skip this chapter and continue with Chapter 7 "Volume Exposure & Security," page 105.

Introduction to V-Switch Clusters

Two V-Switches can be concurrently connected to the same FC storage devices to balance volume exposure thus creating a V-Switch cluster. In a cluster, each V-Switch interacts in an active-active, peer-to-peer fashion with the other V-Switch, or *neighbor*, in the cluster. No one V-Switch must be configured specially to act as the master V-Switch in the cluster providing higher flexibility in building a cluster.

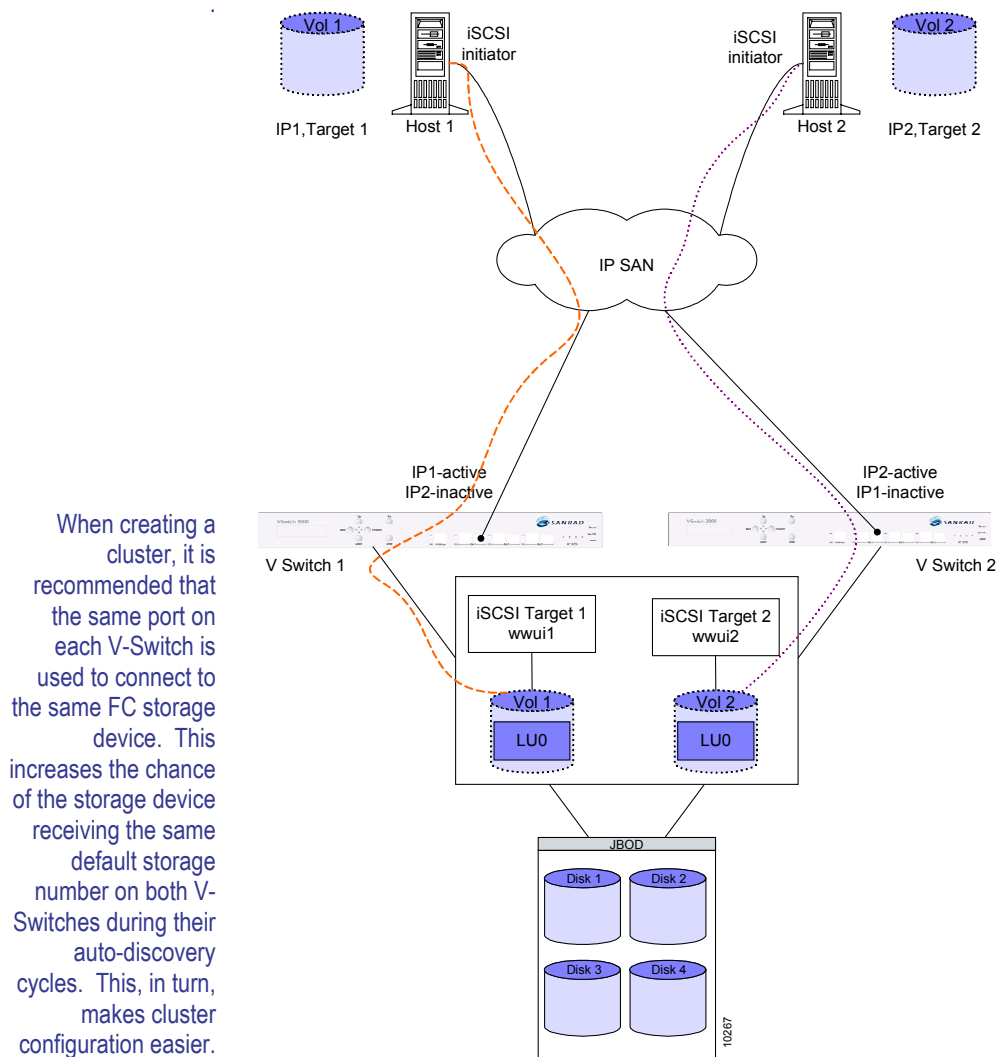
All virtual volumes are accessible to each V-Switch and the exposing V-Switch is defined per volume.

In Figure 32, page 73, two V-Switches are connected to one FC JBOD. From the four physical disks, two virtual volumes have been created, both equally accessible to both V-Switches.

SANRAD V-Switches are both fully operational in a cluster. No V-Switch must sit in stand-by mode.

Both V-Switches are also connected to two hosts via the IP SAN. The volume exposure of the two virtual volumes is balanced equally between the two V-Switches. Volume 1 is exposed via V-Switch 1 to Host 1, represented by the orange dashed line. Volume 2 is exposed via V-Switch 2 to Host 2, represented by the purple dotted line.

The volume exposure is balanced equally between the two V-Switches with one volume exposed on each V-Switch for best resource utilization.



When creating a cluster, it is recommended that the same port on each V-Switch is used to connect to the same FC storage device. This increases the chance of the storage device receiving the same default storage number on both V-Switches during their auto-discovery cycles. This, in turn, makes cluster configuration easier.

Figure 32. V-Switch Cluster Configuration

When working in a cluster, the V-Switch can support a maximum of 100 portals: 50 active and 50 inactive.

Clusters also provide high availability in the event of V-Switch failover. Each network port on the V-Switch is configured with its own active, or functioning, IP addresses as well as inactive, or dormant, neighbor IP addresses. If one V-Switch goes off-line, the remaining V-Switch activates its neighbor's IP addresses. The hosts continue to access volume targets through the same IP address without sensing that their 'regular' V-Switch has gone offline or noticing any impact on storage performance.

When working with FC RAID controllers, it is imperative that all LUNs in the RAID controller are simultaneously exposed through all ports connected to both V-Switches for the V-Switches to provide high availability during a V-Switch failover.

In Figure 33, V-Switch 1 has gone off-line. V-Switch 2 activates V-Switch 1's IP address and takes over exposure of Volume 1 to Host 1, represented by the orange dashed line.

Host 1 continues to access Volume 1 through the same IP address as it did before its V-Switch went off-line. Host 1 has no way of knowing that its regular V-Switch is off-line. Host 1's storage performance is not impacted by the off-line V-Switch.

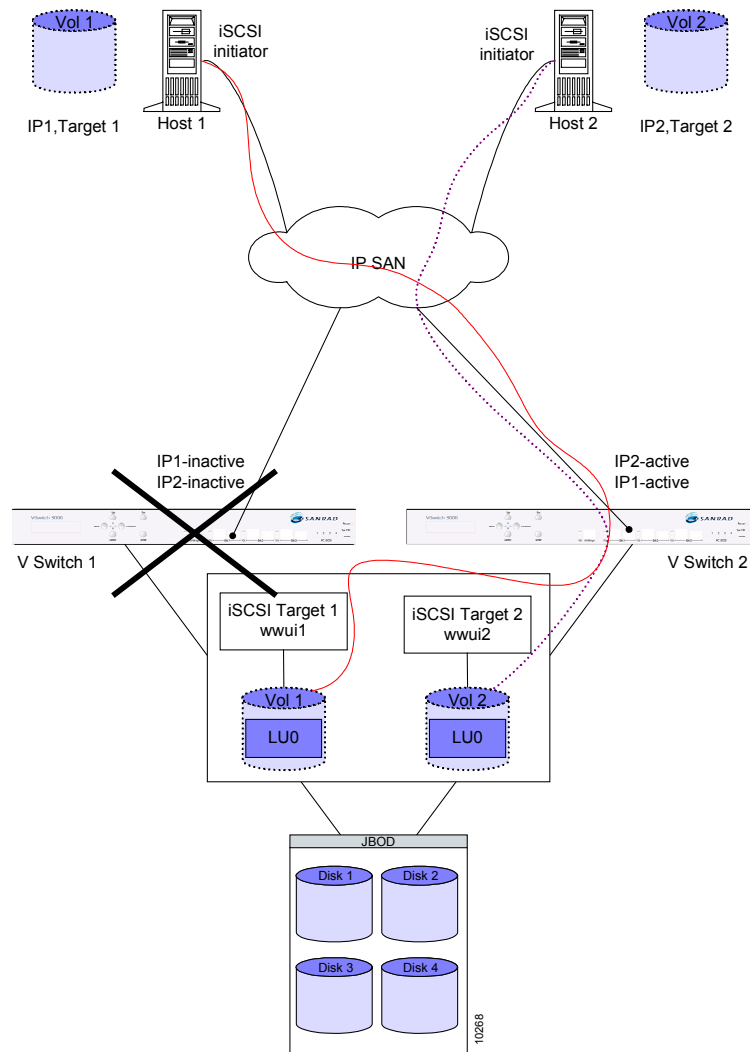


Figure 33. Re-routing Storage Access with Off-line V-Switch

Configuring a V-Switch Cluster

Setting the V-Switch ID

When you configure a cluster, you must give each V-Switch a different device ID for proper cluster functioning. Use the CLI command `device set` to configure the V-Switch ID for each V-Switch.

```
device set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	V-SWITCH ID	ID OF V-SWITCH IN A CLUSTER EACH V-SWITCH MUST HAVE A DIFFERENT ID	MANDATORY IN A CLUSTER 0 OR 1	1

Example:

There are two V-Switches in a cluster. In V-Switch 1 the ID is set to 1.

```
device set -id 1
```

In V-Switch 2 the ID is set to 0.

```
device set -id 0
```

Adding a Neighbor

All CLI names and aliases are case sensitive.

When you configure a cluster, you must tell each V-Switch that it has a neighbor and how to contact its neighbor. Use the CLI command `neighbor add` to inform each V-Switch of its neighbor.

You must inform each V-Switch of its neighbor in a cluster. That means that you must tell V-Switch 1 of V-Switch 2 and V-Switch 2 of V-Switch 1.

When creating a cluster, first ensure that you have configured all IP addresses in the correct active/inactive phase as well as portals and IP routes on both V-Switches. For more information on configuring the V-Switch, see "V-Switch Configuration," page 47.

`neighbor add`

You need to define two parameters to notify a V-Switch of a neighbor.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-nb</code>	NEIGHBOR	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	<code>VSwitch2</code>
<code>-ip</code>	IP ADDRESS	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	<code>212.199.43.75</code>

Example:

A V-Switch is informed that it has a neighbor, VSwitch2, and that it can establish communication with VSwitch2 via IP address 212.199.43.75.

```
neighbor add -nb VSwitch2 -ip 212.199.43.75
```

All V-Switch database configurations must be replicated in both V-Switches when creating a V-Switch cluster, including IP addresses, portals, IP routes, volumes and targets.

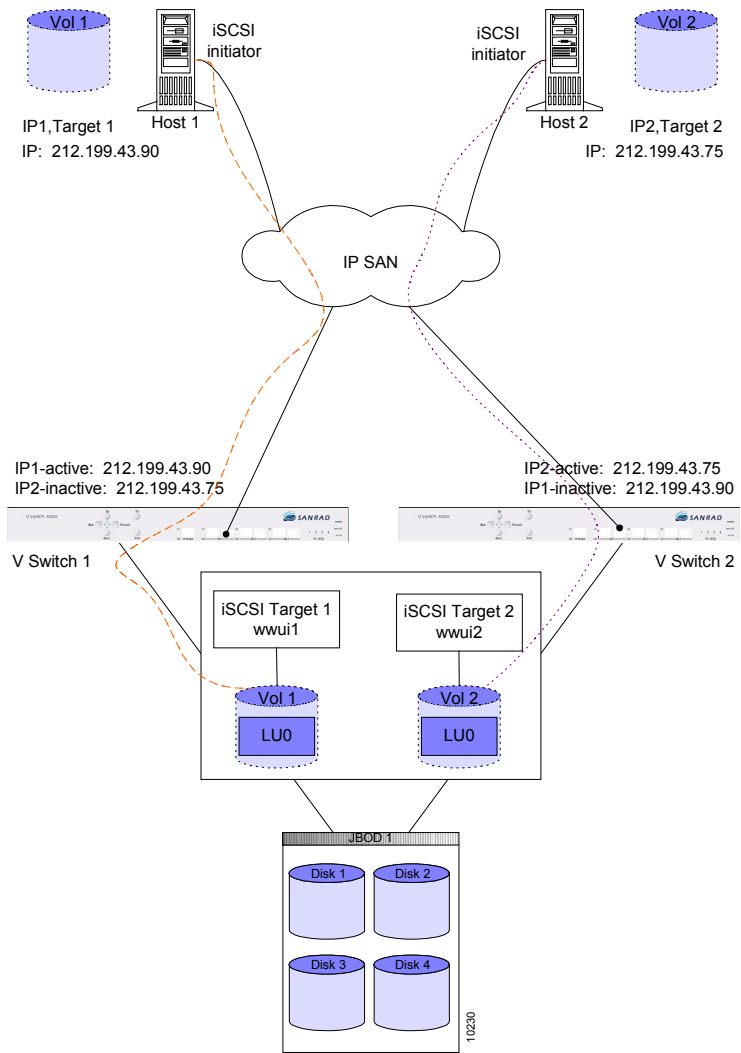


Figure 34. Cluster with Neighbor IP Addresses

Working with SCSI Storage Devices

The V-Switch default SCSI bus ID is 7. If your storage cluster includes SCSI storage devices, one of the V-Switch's default SCSI bus ID must be changed. They cannot both be 7 on the same SCSI bus. Use the CLI command `pscsi set busid` to change the SCSI bus ID on one of the V-Switches.

```
pscsi set busid
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE	STORAGE PORT NUMBER/ALIAS	MANDATORY	<code>pscsi3</code>
-id	ID	PSCSI ID NUMBER BETWEEN 0 AND 15	MANDATORY	<code>12</code>

Example

```
pscsi set busid if pscsi3 -id 12
```

Maintaining Cluster Communications

Once a V-Switch knows that it has a neighbor, it begins sending out a regular *keep alive* signal to its neighbor that it is on-line. The V-Switch also begins listening for the keep alive signal from its neighbor. The keep alive signal is transmitted through all connecting paths between each neighbor. Thus, if one path fails, the remaining path(s) will still carry the keep alive signal.

If a specified time period passes without a keep alive signal from the neighbor, a *suspicious interval*, measured in seconds, is entered. The V-Switch suspects that its neighbor has gone off-line and begins preparing to activate the neighbor IP addresses to take over volume exposure.

If a keep alive signal is received during the suspicious interval, the timer is reset and the V-Switch continues to function as usual. If a keep alive signal is not received by the end of the suspicious interval, a *dead interval* is entered. At the end of the dead interval, the neighboring V-Switch is considered off-line, the failover process is initiated and the on-line V-Switch activates the neighbor IP addresses and takes over volume exposure.

Use the CLI command `cluster show` to view the keep alive parameters of a cluster.

```
cluster show
```

Last Keep Alive	KeepAlive Int(s)	Susp Int(s)	Dead Int(s)
1	2	6	10

Example:

Every 2 seconds V-Switch 1 sends out a keep alive signal. If, after 6 seconds from the last keep alive signal, V-Switch 1 does not receive another keep alive signal from its neighbor, it enters a suspicious interval. If, after 10 seconds from the last keep alive signal, V-Switch 1 enters a dead interval and begins activating the failover process.

Enabling and Disabling Failover

Once you have configured your cluster parameters, you need to enable the failover functionality. Use the CLI command **cluster failover enable** to enable this functionality. This command must be executed on both V-Switches in the cluster.

```
cluster failover enable
```

If you want to break a cluster or need to take a V-Switch off-line, you must first disable V-Switch failover. Use the CLI command **cluster failover disable** to disable this functionality. This command must be executed on both V-Switches in the cluster.

```
cluster failover disable
```

Further V-Switch Cluster Configurations

After configuring neighbor parameters on each V-Switch, you need to configure identical volume configuration and exposure details on each V-Switch in the cluster. Please refer to “Volume Configuration,” page 81, for information on configuring volumes. Please refer to “Volume Exposure & Security,” page 105, for information on exposing volumes.

Please refer to “Configuring a Cluster,” page 272, for a working example of a full cluster configuration.

Viewing V-Switch Neighbor Details

Use the CLI command `neighbor show` to view the neighbor configured on a V-Switch.

```
neighbor show
```

Table 16: Neighbors in a Cluster

Name	IP Address	UDP	SNMP Timeout (msec)	SNMP # of Retries
VSwitch2	212.199.43.75	161		

Use the CLI command `neighbor details` to list the details of a neighbor in a cluster.

```
neighbor details
```

You need to define one parameter to list neighbor details.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBOR IN CLUSTER	MANDATORY	VSwitch2

Table 17: Neighbor Details

Neighbor Name	VSwitch2
IP Address	212.199.43.75
Last Received Keep Alive:	3
Status	Alive
Lock Status	srOpen

A neighbor's status can be alive, suspicious or dead. The lock status can be open, master lock or slave lock. The lock status is not currently configurable and the default status is open.

Managing a Cluster

If you modify a V-Switch alias or management IP address, you must implement the updates in the neighboring V-Switch. Use the CLI command **neighbor set** to update a V-Switch on changes in its neighbor.

neighbor set

You need to define the parameter(s) to modify to reset a neighbor alias or IP address in a cluster.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR ALIAS	NEIGHBORING V-SWITCH IN CLUSTER	OPTIONAL	VSwitch2
-ip	NEIGHBOR MANAGEMENT IP ADDRESS	MANAGEMENT IP OF THE NEIGHBORING V-SWITCH	OPTIONAL	212.199.43.75

Use the CLI command **neighbor remove** to remove a neighbor from a cluster.

neighbor remove

You need to define two parameters to remove a neighbor.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR ALIAS	NEIGHBORING V-SWITCH IN CLUSTER	MANDATORY	VSwitch2
-ip	NEIGHBOR MANAGEMENT IP ADDRESS	MANAGEMENT IP OF THE NEIGHBORING V-SWITCH	MANDATORY	

Use the CLI command **cluster set** to modify the default keep alive intervals.

cluster set

You need to define the parameters you want to modify in the keep alive interval.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-kai	KEEP ALIVE INTERVAL	TIME BETWEEN ALIVE SIGNALS FROM NEIGHBORS	OPTIONAL DEFAULT: 2 SEC	5
-sint	SUSPICIOUS INTERVAL	TIME FROM WHEN A SIGNAL WAS EXPECTED BUT NOT RECEIVED	OPTIONAL DEFAULT: 6 SEC	10
-fint	FAILOVER INTERVAL	TIME WHEN SUSPICIOUS INTERVAL IS EXCEEDED	OPTIONAL DEFAULT: 10 SEC	10



Volume Configuration

IN THIS CHAPTER

INTRODUCTION TO VOLUME CONFIGURATION

IDENTIFYING AVAILABLE STORAGE DEVICES

CREATING A TRANSPARENT VOLUME

CREATING A SUBDISK (LUN CARVING)

CREATING A SIMPLE VOLUME

CREATING A CONCATENATED VOLUME

CREATING A STRIPED VOLUME

CREATING A MIRRORED VOLUME

CREATING A RAID 10 AND RAID 0+1

After you have configured the V-Switch general parameters, you can begin defining the storage topology using the Volume Manager.

Using the Volume Manager, you can create subdisks on physical disk storage devices or leave the physical disk as is. These physical volumes can then be used to create the following types of virtual volumes:

- ❑ Transparent
- ❑ Simple
- ❑ Concatenated
- ❑ Striped
- ❑ Mirrored
- ❑ RAID 10 and 0+1

Introduction to Volume Configuration

This chapter describes how to identify the SAN storage devices and use them to create subdisks and virtual volumes. Each description includes:

- A general description and generic diagram.
- The basic command, switches and parameters needed to execute the command.
- An example of how to use the command with an accompanying diagram.

The specific examples used in this chapter contain two JBODs; each JBOD having four disks, each with a volume of 18 GB. See the example in Figure 35.

The Volume Manager names all disks automatically during the auto-discovery process. For FC, this name includes FC disk's *World Wide Unique Identifier (WWUI)* serial number. For SCSI, this name includes the SCSI disk port number and SCSI bus ID. This name is important in identifying disks for re-creating volume hierarchies on both V-Switches in a cluster.

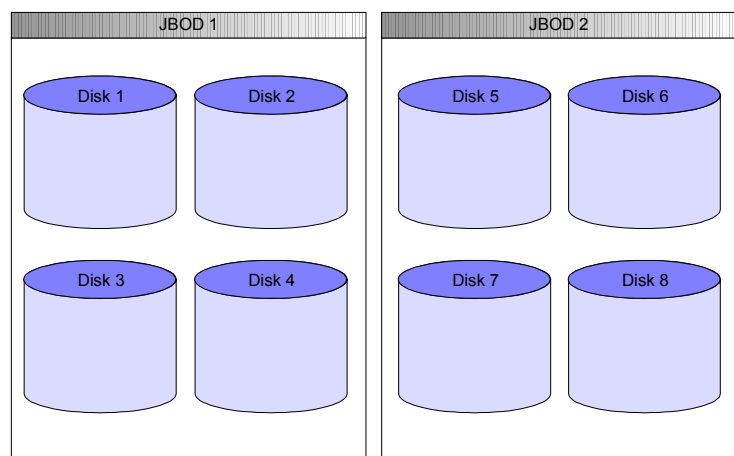


Figure 35. Physical Storage used in Examples

If you are working in a V-Switch cluster, you need to configure all subdisks and volumes on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

Identifying Available Storage Devices

The V-Switch supports a maximum of 512 disks.

Before beginning to configure virtual volumes, you need to know which storage devices are available. Use the CLI command **storage show** to show the available storage devices and their corresponding aliases needed to configure volumes

```
storage show
```

Table 18: Storage Devices

Alias	Entity Name	LUN	Oper. Status	Type
Stor_1	500507606058c900	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire

Enabled operating status denotes an attached and functioning storage device. Storage is missing denotes that a storage device was previously registered and has since lost its connection to the V-Switch.

If a subdisk has been created on a disk, the subdisk status in the disk details will display split. If no subdisks were created, the subdisk status will display entire. See “storage details,” page 87.

Not all storage devices are able to support this feature.

The V-Switch automatically generates and assigns storage aliases as each device is discovered. Use the CLI command **storage blink activate** to identify the actual physical device for an alias.

```
storage blink activate
```

You need to define two parameters to blink a storage device:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE DEVICE	ALIAS OF DEVICE TO BLINK	MANDATORY	Stor_1
-t	TIME	LENGTH OF TIME TO BLINK DEVICE	OPTIONAL 1-3600 SEC 0=FOREVER DEFAULT: 0	120

Example:

The storage device, Stor_1, is set to blink for two minutes (one hundred and twenty seconds) to allow it to be identified.

```
storage blink activate -s Stor_1 -t 120
```

Use the CLI command **storage blink abort** to stop the blinking before the end of the set time.

```
storage blink abort
```

You need to define one parameter to stop blinking a storage device:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE DEVICE	ALIAS OF DEVICE TO BLINK	MANDATORY	Stor_1

Once a storage device has been identified, use the CLI command **storage set** to change the device alias or include helpful information on the device.

```
storage set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE ALIAS	STORAGE ALIAS TO MODIFY	MANDATORY	Stor_1
-na	NEW ALIAS	NEW ALIAS FOR STORAGE	OPTIONAL	Disk2JBOD5
-info	INFORMATION	INFORMATION ON STORAGE TO SET	OPTIONAL	save_for_snapshots

Example:

The alias of Stor_1 is changed to Disk2JBOD5 for easier identification and it is noted to save the disk for snapshots.

```
storage set -s Stor_1 -na Disk2JBOD5 -info save_for_snapshots
```

The V-Switch supports write cache enabling for increased performance. Use the CLI command **storage disk set** to enable or disable the write cache.

```
storage disk set
```

You need to define two parameters to change a device's write cache setting:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-d	DISK	DISK DEVICE	MANDATORY	Disk2JBOD5
-wce	WRITE CACHE ENABLED	WRITE CACHE FUNCTION	MANDATORY YES OR NO	yes

The V-Switch also recognizes all write-protected storage devices. Use the CLI command `storage details` to view a device's details, including if it is write-protected.

`storage details`

You need to define one parameter to view a disk's details:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE	ALIAS OF STORAGE TO VIEW	MANDATORY	Disk2JBOD5

Table 19: Storage Details

Alias:	Disk2JBOD5
Entity Name:	2000002037a9551e
LUN(Logical Unit Number)	0000000000000000
Vendor Name:	SEAGATE
Additional Info:	
Transport type:	Fiber Channel
Oper. Status:	Enabled
Time since last Update:	8 days 3h:12m:16 sec 37 (1/60 Sec)
SCSI Version:	3
Revision Level:	0002ST336704FC
Product Id:	ST336704FC
Serial Number:	3CD0FHA400002108XYGLXYGL
Number Of Blocks:	71687369
Block Size:	512
SubDisks:	Entire
Write Cache Enabled:	true
Write Protected	false
Volume	sim

Creating a Transparent Volume

Transparent volumes cannot be used in further volume hierarchies.

You can take a physical disk and its existing configured storage data and convert it to a directly accessible, or transparent, virtual volume using the CLI command `volume create transparent`. A transparent volume is ready for direct host exposure. Please refer to “Volume Exposure & Security,” page 107.

Tape devices must be virtualized as transparent volumes.

Certain vendor storage devices have vendor-specific SCSI commands. To support these SCSI commands, you can convert these storage devices and their contained data to transparent volumes.

This is useful if you have a functioning and fully configured RAID module that you want to use ‘as is’. All RAID configurations will be maintained in the transparent volume.

`volume create transparent`

You need to define two parameters to create a transparent volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME ALIAS	USER-ASSIGNED ALIAS FOR THE VOLUME	OPTIONAL DEFAULT: STORAGE ALIAS	Trans1
<code>-d</code>	DISK ALIAS	ALIAS GIVEN TO THE DISK DURING DISK AUTO-DISCOVERY	MANDATORY	Disk1

Example:

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure 36, page 89, the logical unit, LUN0 on Disk 1, is converted directly to a virtual transparent volume, Transparent 1. This RAID device has only one LUN. For each LUN configured on a RAID device, the V-Switch registers a disk. Therefore, a RAID device with five LUNs will appear to the V-Switch as five disks.

```
volume create transparent -vol Trans1 -d Disk1
```

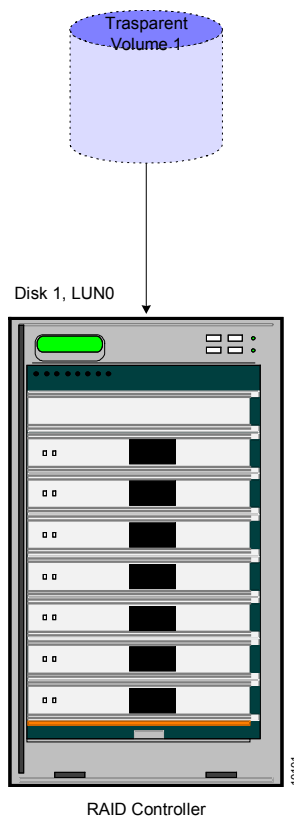


Figure 36. Transparent Volume 1

After creating the transparent volume, you can use the CLI command `volume show` to verify the volume creation.

```
volume show
```

Table 20: Volume Details

Alias	Vol Type	# of Blocks	Block Size	State
Trans1	Transpar	1024	512	Internal

Creating a Subdisk (LUN Carving)

The V-Switch supports a maximum of 512 subdisks.

You can create one or more subdisks on a physical disk. The subdisks can then be converted to simple volumes to be used for creating concatenated, striped and mirrored virtual volumes. When you create a subdisk, only the defined area is converted into a subdisk. You must individually convert each disk area into a subdisk for the physical volume to be usable by the Volume Manager.

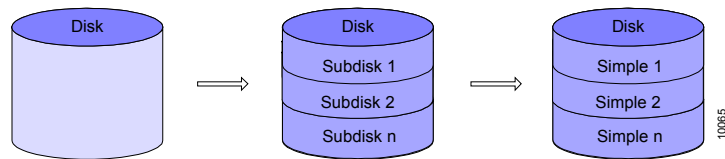


Figure 37. Partitioning a Physical Volume

`subdisk create`

You need to define four parameters to create a subdisk

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-d</code>	DISK ALIAS	ALIAS OF DISK TO SPLIT	MANDATORY	Disk1
<code>-sl</code>	SPLIT LENGTH	LENGTH IN Blocks OF SUBDISK	MANDATORY (1 BLOCK = 512 BYTES)	18000000
<code>-sa</code>	START ADDRESS	BLOCK TO BEGIN COUNTING THE SUBDISK LENGTH FROM	OPTIONAL DEFAULT: 0	0
<code>-sd</code>	SUBDISK ALIAS	USER-ASSIGNED ALIAS FOR SUBDISK	OPTIONAL DEFAULT: DEF_SPLIT_ CLUSTER NO_ DISK NO_END ADDRESS IN BLOCKS	Subdisk1

Example:

In Figure 38, page 91, you see Disk 1 before a subdisk is created on it.



Figure 38. Disk 1 before Subdisk

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure **Error! Bookmark not defined.**, page **Error! Bookmark not defined.**, Subdisk 1 has been created on Disk 1. The subdisk is 18,000,000 blocks long (9 GB). The Volume Manager begins counting the 18,000,000 blocks from block 0.

```
subdisk create -d Disk1 -sl 18000000 -sa 0 -sd Subdisk1
```



Figure 39. Disk 1 with 1 Subdisk

After creating the subdisk, you can use the CLI command **subdisk show** to view it and all configured subdisks. You can use the CLI command **subdisk details** to view the details of the created subdisk.

```
subdisk details
```

You need to define one parameter to view subdisks.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-d	DISK ALIAS	ALIAS OF DISK TO SHOW SUBDISKS FROM	OPTIONAL USE THIS SWITCH TO LIST ONLY THE DETAILS OF A SPECIFIC DISK	Disk1

This command calls up the following table.

Table 21: Details of all Subdisks

Disk	Subdisk	Start Address	Length	Vol
Disk1	Subdisk1	0	512	no

For the rest of the physical volume on Disk 1 to be usable to the Volume Manager, you must create another subdisk.

```
subdisk create -d Disk1 -sl 18000000 -sa 18000000 -sd Subdisk2
```



Figure 40. Disk 1 with 2 Subdisks

Creating a Simple Volume

The V-Switch supports a maximum of 512 volumes.

Before you can build concatenated, mirrored and striped volumes, you must create simple volumes from each disk or subdisk in your storage network.

A physical disk or subdisk is converted directly to a virtual simple volume. A simple volume differs from a transparent volume in that virtual volume hierarchies can be built on top of simple volumes but not on transparent volumes. In Figure 41, data blocks 1 - 4 are mapped to blocks 5 - 8 of Disk 2.

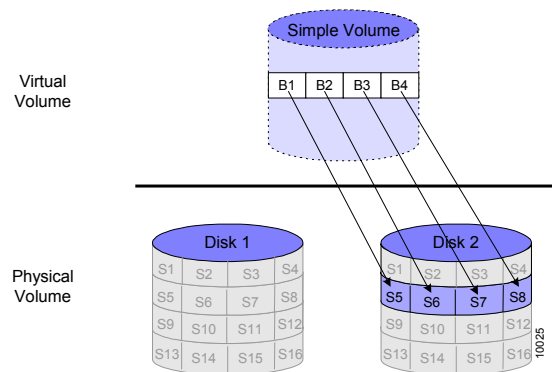


Figure 41. Simple Volume Block Distribution

```
volume create simple
```

You need to define three parameters to create a Simple Volume.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	USER-ASSIGNED NAME FOR SIMPLE VOLUME	OPTIONAL DEFAULT: (SUB)DISK ALIAS	Simple1
-sd	SUBDISK ALIAS	ALIAS OF THE SUBDISK IN WHICH TO CREATE THE VOLUME – IF THE PHYSICAL DISK WAS DIVIDED INTO SUBDISKS	MANDATORY ASSIGN AN ALIAS TO EITHER A DISK OR A SUBDISK	Subdisk1
-d	DISK ALIAS	ALIAS OF THE DISK IN WHICH TO CREATE THE VOLUME	MANDATORY ASSIGN AN ALIAS TO EITHER A DISK OR A SUBDISK	

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

Assigning a volume alias is optional. If you do not include a volume alias in the command, the volume alias will default to the subdisk alias in which the volume is located. For example, a simple volume created on Subdisk 6 will be named Subdisk 6 by default.

Use the `-sd` switch to assign a subdisk or the `-d` switch to assign a disk.

Example:

In Figure 42, Subdisk 1 on Disk 1 is converted to a simple volume, Simple 1.

```
volume create simple -vol Simple1 -sd Subdisk1
```

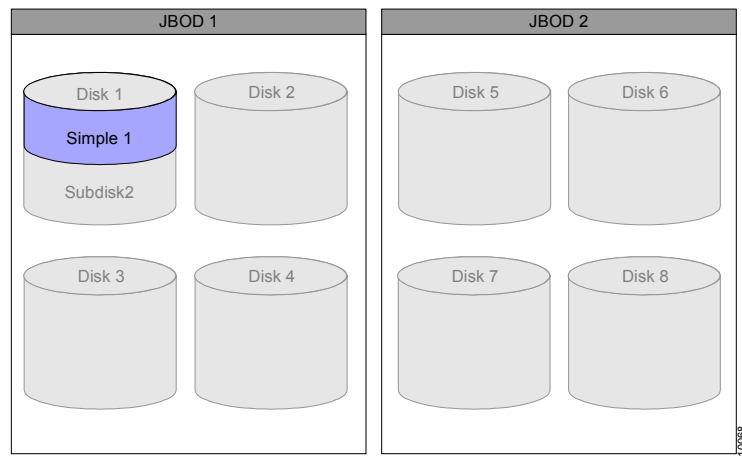


Figure 42. Simple Volume 1

Use the CLI command `volume show` to show the created volume:

```
volume show
```

Alias	Type	Act # of Bl	Pot # of Bl	B1 Size	State
Simple1	Simple	17999999	17999999	512	Internal

Creating a Concatenated Volume

The V-Switch supports a maximum of 512 volumes.

To accommodate large volumes of data or to best utilize small volumes spread over several disks, you can concatenate physical volumes across storage devices to create a larger virtual volume.

In Figure 43, the volume is divided into two equitable chunks to be mapped across two disks. Data blocks 1 - 4 are mapped to Disk 1, blocks 13 - 16. Data blocks 5 - 8 are mapped to Disk 2, blocks 13 - 16.

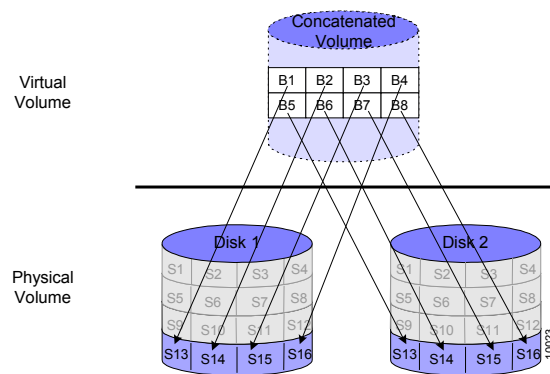


Figure 43. Concatenated Volume Block Distribution

```
volume create concatenated
```

You need to define four parameters to create a concatenated volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME NAME	USER-ASSIGNED VOLUME NAME	MANDATORY	Concat1
-nbc	NUMBER OF CHILDREN	NUMBER OF VOLUMES OR CHILDREN FROM WHICH TO BUILD STRIPED VOLUME	OPTIONAL DEFAULT: 2	3
-ch	CHILD	FIRST VOLUME (CHILD) TO COMBINE	MANDATORY	Simple5
-ch	CHILD	SECOND VOLUME (CHILD) TO COMBINE	MANDATORY	Simple12
-ch	CHILD	N VOLUME (CHILD) TO COMBINE	MANDATORY	Simple14

The system default for the number of children being concatenated is two. Therefore, you only need to specify the number of children for numbers greater than two.

Example:

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure 44, Simple Volume 5 and Simple Volume 12, both built over an entire physical disk, are concatenated to create a concatenated volume, Concat 1. Data is read/written first to Simple 5. When the data chunk gets to the end of Simple 5, it continues with Simple 12 reflecting the volume order as entered in the CLI command.

```
volume create concatenated -vol Concat1 -ch Simple5 -ch Simple12
```

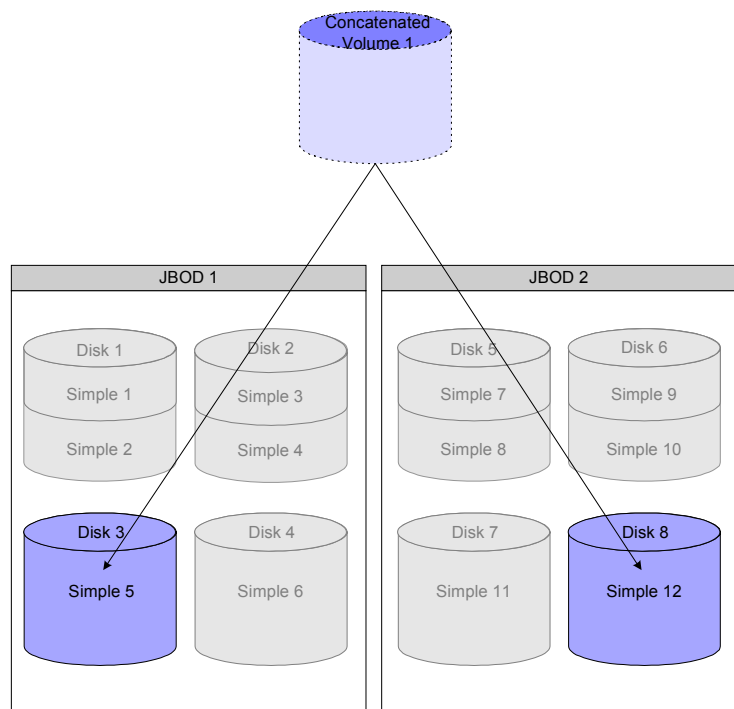


Figure 44. Concatenated Volume 1

Creating a Striped Volume

The V-Switch supports a maximum of 512 volumes.

A striped volume has data written equitably across two or more disks to provide higher read/write rates. Subdisks within a striped volume need to be on different disks to realize the benefits of striping. Throughput increases with the number of disks within a striped volume.

In Figure 45, data block 1 is mapped to section 1 of Disk 1; data block 2 is mapped to block 1 of Disk 2. Each subsequent data block is then written alternately between blocks on Disks 1 and 2. The striped unit size in this example is one block.

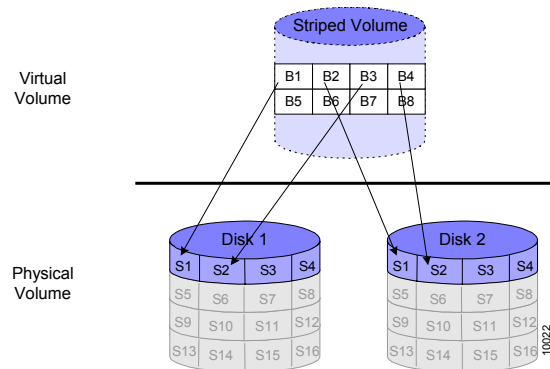


Figure 45. Striped Volume Block Distribution

```
volume create stripe
```

You need to define four parameters to create a striped volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME ALIAS	USER-GIVEN ALIAS FOR VOLUME CREATED	OPTIONAL DEFAULT: (SUB)DISK ALIAS	Stripe1
<code>-sus</code>	STRIPE UNIT SIZE	NUMBER OF BLOCKS READ/Written INTO EACH VOLUME BEFORE MOVING ON TO THE NEXT CHILD IN THE STRIPE	MANDATORY	100
<code>-nbc</code>	NUMBER OF CHILDREN	NUMBER OF VOLUMES OR CHILDREN FROM WHICH TO BUILD STRIPED VOLUME	OPTIONAL DEFAULT: 2	4

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ch	CHILD	FIRST VOLUME (CHILD) TO WRITE TO	MANDATORY	Simple2
-ch	CHILD	SECOND VOLUME (CHILD) TO WRITE TO	MANDATORY	Simple4
-ch	CHILD	THIRD VOLUME (CHILD) TO WRITE TO	MANDATORY	Simple8
-ch	CHILD	FOURTH VOLUME (CHILD) TO WRITE TO	MANDATORY	Simple10

The system default for the number of children data is being striped across is two. Therefore, you only need to specify the number of children for numbers greater than two.

Example:

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure 46, page 99, a striped volume, Stripe 1, is created across four children: Simple 2, Simple 4, Simple 8 and Simple 10. The striped unit size is 100 blocks, meaning that in each read/write function, 100 blocks of data are read/written into Simple 2; then 100 blocks into Simple 4; then 100 blocks into Simple 8; then 100 blocks into Simple 10 and then back again to 100 blocks in Simple 2 until the end of the data chunk.

```
volume create stripe -vol Stripe1 -nbc 4 -sus 100 -ch Simple2 -ch Simple4 -ch Simple8 -ch Simple10
```

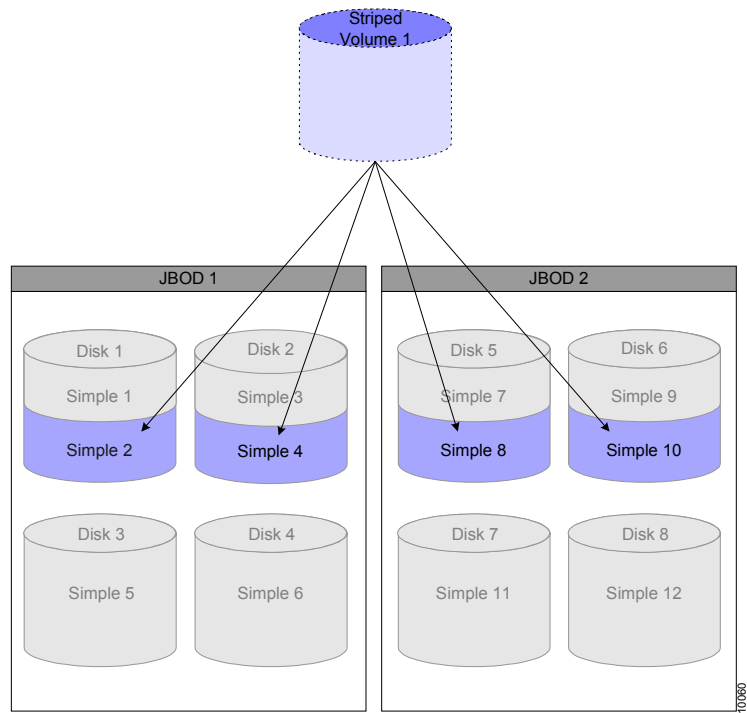



Figure 46. Striped Volume 1

Creating a Mirrored Volume

Use mirroring to create data backups.

The V-Switch supports a maximum of 512 volumes.

A mirrored volume is synchronously written into two or more volumes. Mirrored volumes provide protection against data loss from a physical disk crash. To be a true mirror and realize the full potential of a mirror, the mirrored volumes must be located on different physical disks.

In Figure 47, data block 1 is mapped to both block 5 on Disk 1 and block 9 on Disk 2. Data blocks 2, 3 and 4 are mapped to both blocks 6,7 and 8 on Disk 1 and blocks 10, 11 and 12 on Disk 2.

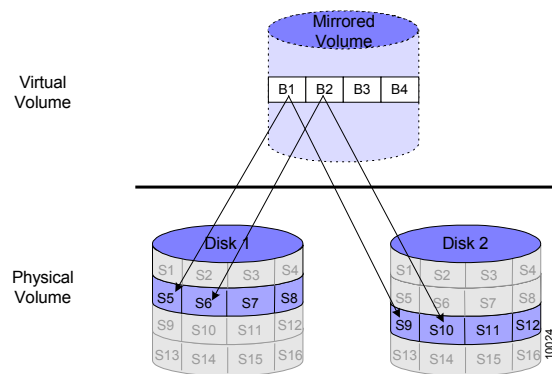


Figure 47. Mirrored Volume Block Distribution

`volume create mirror`

You need to define four parameters to create a mirrored volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME ALIAS	USER-ASSIGNED ALIAS FOR THE MIRRORED VOLUME	MANDATORY	Mirrored1
<code>-nbc</code>	NUMBER OF CHILDREN	NUMBER OF CHILDREN IN MIRRORED VOLUME	OPTIONAL DEFAULT: 2 MAX: 4	
<code>-ch</code>	CHILD	NAME OF EACH CHILD TO INCLUDE IN THE MIRROR	MANDATORY	Simple6
<code>-ch</code>	CHILD	NAME OF EACH CHILD TO INCLUDE IN THE MIRROR	MANDATORY	Simple11

Example:

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure 48, a mirrored volume, Mirrored 1, is created using two children, Simple 6 and Simple 11.

```
volume create mirror -vol Mirrored1 -ch Simple6 -ch Simple11
```

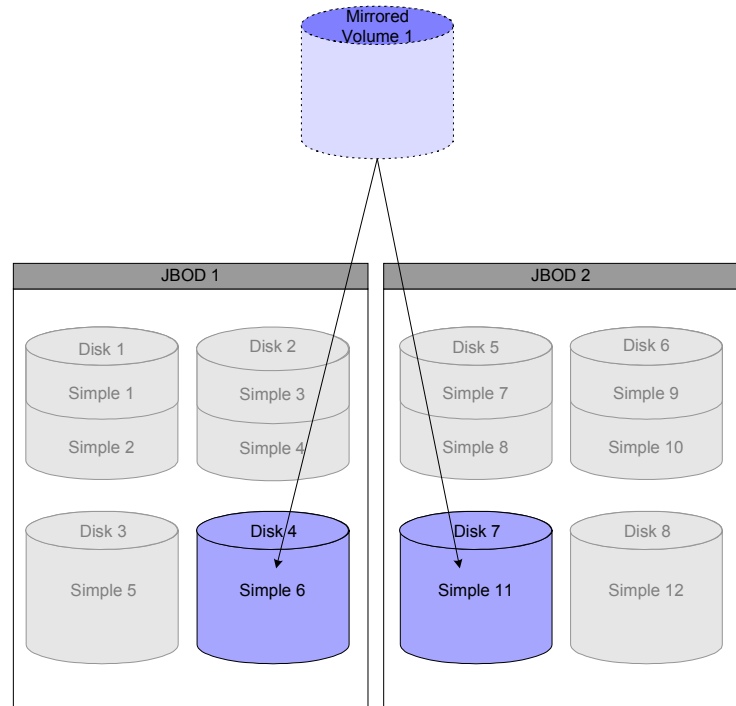


Figure 48. Mirrored Volume 1

Replicating Data in a Mirrored Volume

If one child of a mirrored volume, the source, already contains data, the data can be replicated to the second child, the destination, using the CLI command **volume mirror sync**. This is done on-line while the source volume is still exposed. See how to expose volumes “Volume Exposure & Security,” page 107.

Data can also be replicated offline using the CLI command **volume copy create**. On-line data replication is slower but allows the source volume to remain on-line with no interruption of service to the volume host(s). Off-line replication is faster than on-line replication but both the source and destination volumes must be off-line which can create an interruption of service to the volume host(s).

See the working example of off-line data replication “Replicating Data Off-line,” page 264.

volume mirror sync

You need to define two parameters to synchronize a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE VOLUME	ORIGINAL VOLUME TO SYNCHRONIZE TO	MANDATORY	Simple3
-dst	DESTINATION VOLUME	NEW VOLUME TO ADD TO SYNCHRONINZE	MANDATORY	Simple5

Example:

The online volume Simple3 is synchronized to the online volume Simple5.

volume mirror sync -src Simple3 -dst Simple5

Creating a RAID 10 and RAID 0+1

You will need two separate commands to create a RAID 10 or 0+1 volume. RAID 10 first creates mirrored volumes and then creates a striped volume of the mirrored volumes. This gives the advantage of both high performance and data redundancy.

In Figure 49, page 104, in the first mirrored volume, data block 1 is mapped to both block 1 on Disk 1 and block 1 on Disk 2. Data blocks 3, 5 and 7 are mapped to blocks 2, 3 and 4 on both Disks 1 and 2.

In the second mirrored volume, data block 2 is mapped to both block 1 on Disk 3 and block 1 on Disk 4. Data blocks 4, 6 and 8 are mapped to blocks 2, 3 and 4 on Disks 3 and 4.

Data blocks 1 and 2 are then compiled in a striped pattern, along with blocks 3 – 8.

RAID 0+1 first creates striped volumes and then creates mirrored volumes of the striped volumes.

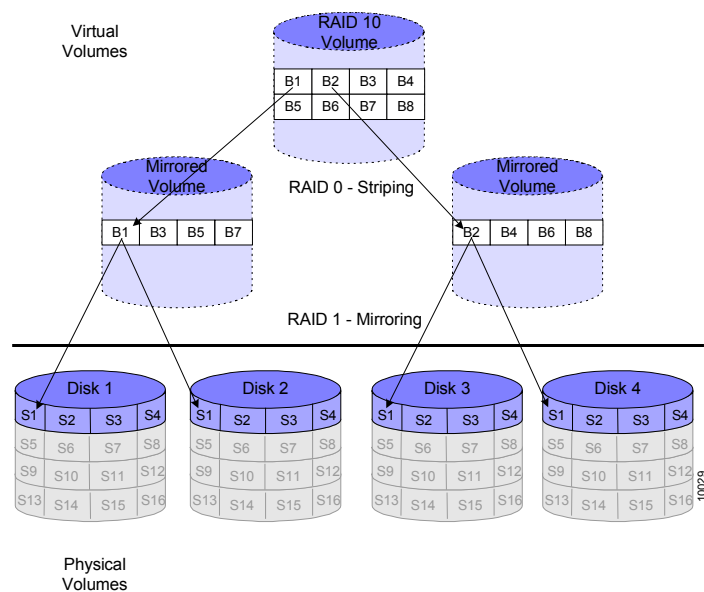


Figure 49. RAID 10 Volume Block Distribution

Example:

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

In Figure 51, page 105, to begin creating a RAID 10 volume, a mirrored volume, Mirror 2, is created using two children: Simple 1 and Simple 7.

```
volume create mirror -vol Mirror2 -ch Simple1 -ch Simple7
```

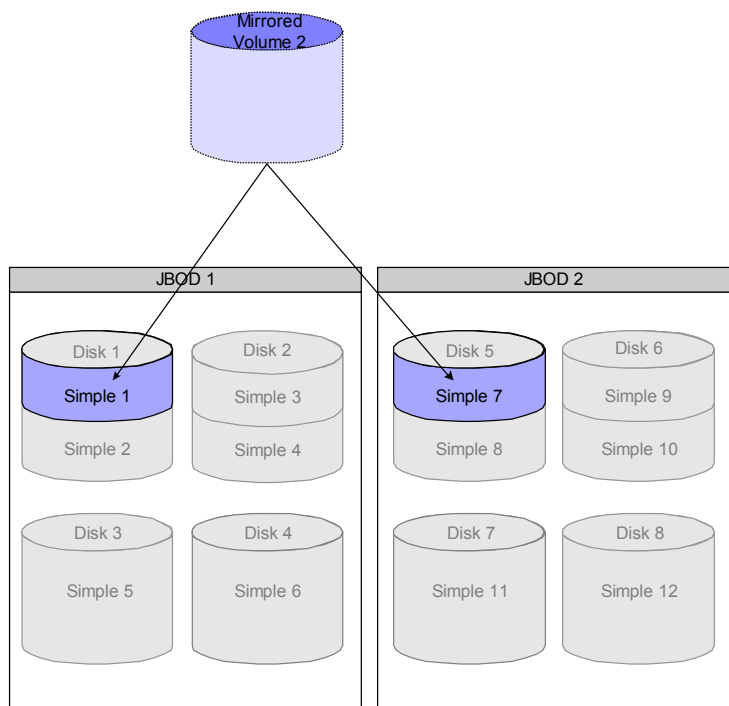


Figure 50. First Mirrored Volume of RAID 10

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

Next, in Figure 51, page 105, another mirrored volume, Mirror 3, is created using two children: Simple 3 and Simple 9.

```
volume create mirror -vol Mirror3 -ch Simple3 -ch Simple9
```

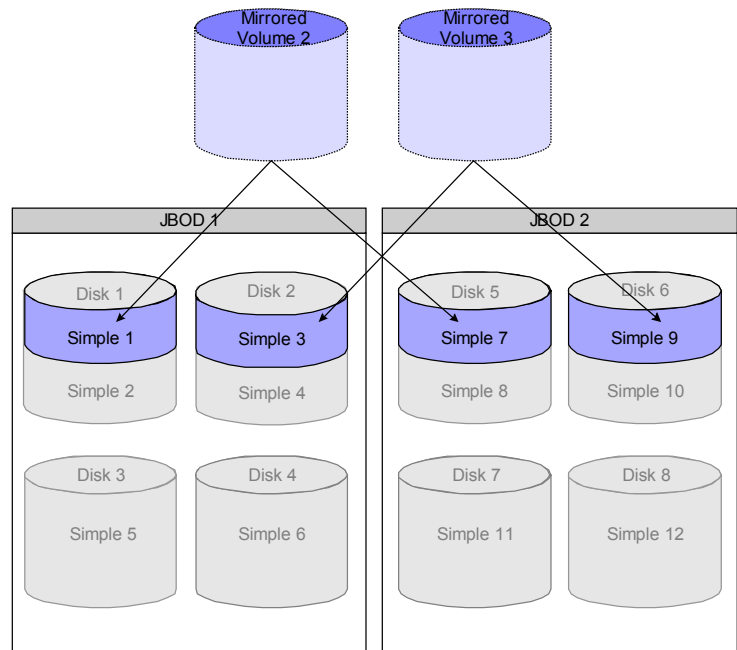


Figure 51. Second Mirrored Volume of RAID 10

If you are working in a V-Switch cluster, this volume must be configured on both V-Switches.

Finally, in Figure 52, page 106, a striped volume, Stripe 2, is created using the two mirrored volumes as children: Mirror 2 and Mirror 3. The striped unit size is 100 blocks, meaning that in each read/write function, 100 blocks of data are read/written first into Mirror 2 then Mirror 3 and then back to Mirror 2 until the end of the data chunk.

```
volume create stripe -vol Stripe2 -sus 100 -ch Mirror2 -
ch Mirror3
```

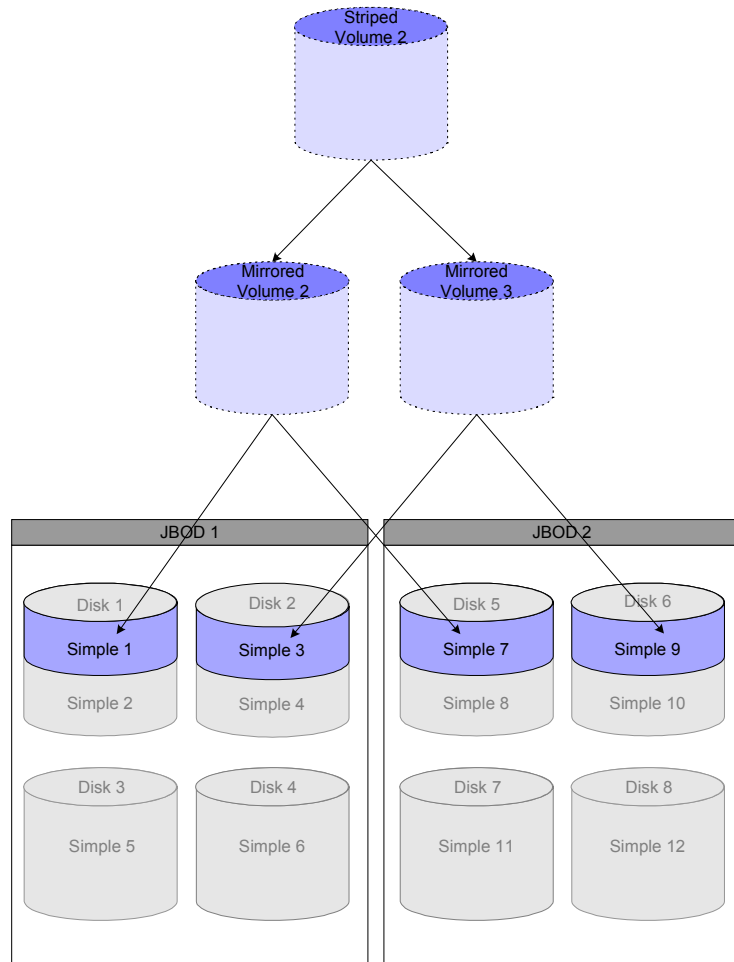


Figure 52. Striped Volume of RAID 10

To create a RAID 0+1 volume, invert the commands and first create a striped volume and then mirrored volumes of the stripe.



7

Volume Exposure & Security

IN THIS CHAPTER

INTRODUCTION TO VOLUME EXPOSURE & SECURITY

After you have created your virtual volumes and storage hierarchies, you want to expose them securely to hosts using the iSCSI protocol. Up to this point, all volumes created are invisible and inaccessible to network hosts.

CREATING AN iSCSI TARGET

This chapter explains how to create iSCSI *targets*; assign *LUNs* to volumes and attach LUNs to iSCSI targets. This enables hosts with installed iSCSI initiators to view and access the exposed volumes.

CHANGING THE DEFAULT IDENTITY

This chapter also explains how to create *identities*, assign access rights and enable *authentication methods* to control iSCSI initiator access to exposed volumes.

CREATING AN IDENTITY

ADDING INITIATORS TO AN IDENTITY

ASSIGNING IDENTITY CREDENTIALS

CONNECTING AN IDENTITY AND TARGET

EXPOSING AN iSCSI TARGET AND LUN

Introduction to Volume Exposure & Security

iSCSI Targets

Data is able to be transferred via iSCSI when an iSCSI initiator establishes a TCP connection with an iSCSI target.

- The iSCSI initiator resides in the host computer and is configured by the system administrator.
- The iSCSI target resides in the V-Switch and is created by the volume manager.

To enable iSCSI communications over TCP, the system administrator configured portals during the initial V-Switch configuration, consisting of a network port IP address and its assigned TCP port. Please see “Configuring iSCSI Portals,” page 64 for more details. Each configured portal is automatically attached to all iSCSI targets created. Typically, there are few portals and many targets.

Both iSCSI initiators and targets have a *World Wide Unique Identifier* (WWUI) of up to 256 free form characters, e.g. `www.sanrad.vswitch1.target1`.

You create a V-Switch target by assigning an alias and WWUI to it.

You assign a *Logical Unit Number* (LUN) to a volume and then attach the LUN to an iSCSI target to expose the volume to hosts.

When creating targets, keep in mind that:

- Each target can have multiple LUNs.
- Each target must have LU0 to be functional.
- Each target should be exposed by only one V-Switch in a cluster.
- Each target can be accessed by multiple hosts.

There are two ways to create a LUN and target:

- Assign a LUN and create a target together.
- Create targets first and later assign LUNs to the pre-created targets.

The V-Switch in Figure 53, page 109, contains three iSCSI targets: Target 1, Target 2 and Target 3. It has two portals: (IP1, 5003) and (IP2, 5003). Target 1 and Target 2 have only one volume attached to each. Therefore, each volume is automatically assigned LU0. Target 3 has two attached volumes, LU0 and LU1.

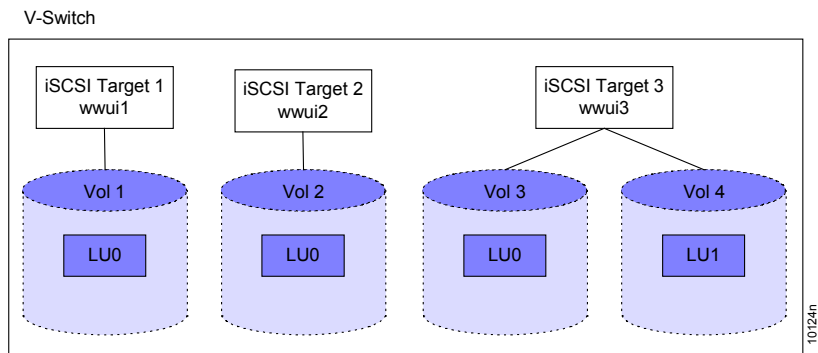


Figure 53. iSCSI Target Access

Once a volume has a LUN and is attached to a target, it is accessible to iSCSI initiators. Each initiator can access, read and write into the volume.

Identities

To allow selective iSCSI initiator access to iSCSI target volumes, the V-Switch uses *identities* to define pools of initiators. An identity is a user-defined list of iSCSI initiators. An identity can contain from one to multiple initiators, with each initiator having a unique WWUI.

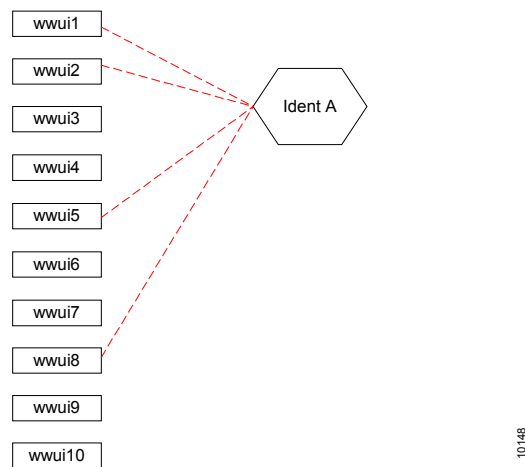
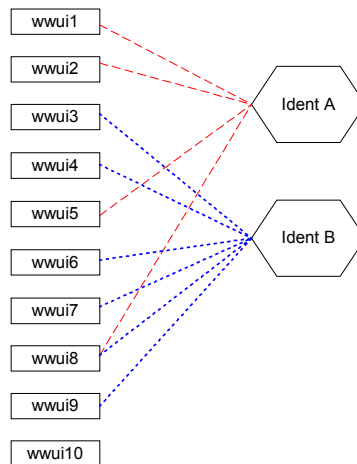


Figure 54. Identity A's iSCSI Initiators

In Figure 54, there are four iSCSI initiators in Identity A: WWUI 1, 2, 5 and 8.

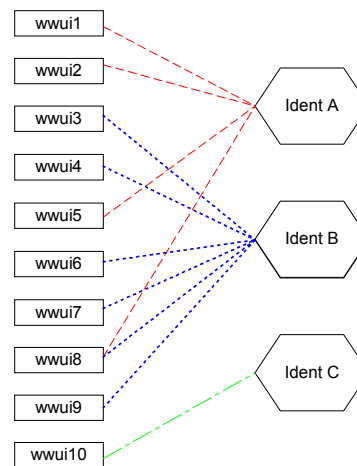
An iSCSI initiator can be listed in multiple identities.



10149

Figure 55. Identity B's iSCSI Initiators

In Figure 55, there are six iSCSI initiators in Identity B: WWUI 3, 4, 6, 7, 8 and 9. Note that iSCSI initiator 8 is in both Identity A and B. An iSCSI initiator can be listed in multiple identities.



10150

Figure 56. Identity C's iSCSI Initiator

In Figure 56, there is only one iSCSI initiator in Identity C: WWUI10.

Identities are coupled with iSCSI targets to limit iSCSI initiator access to a target's underlying volumes. An identity can be used with more than one target and each target can have more than one identity.

An identity can be used with more than one target.

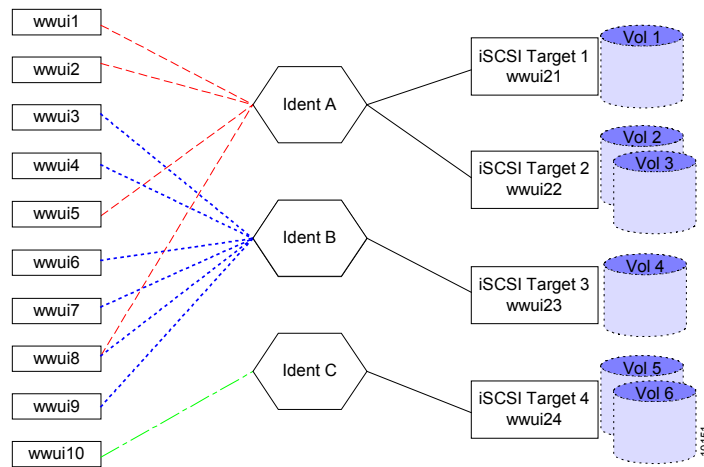


Figure 57. Identities Coupled with Targets

In Figure 57, Identity A is coupled with both Targets 1 and 2. Identity B is coupled with Target 3. Identity C is coupled with Target 4. As a result, each iSCSI initiator has access to the following volumes:

iSCSI INITIATOR	VOLUMES ACCESSIBLE			
WWUI1	▶VOL1	▶VOL2	▶VOL3	
WWUI2	▶VOL1	▶VOL2	▶VOL3	
WWUI3	▶VOL4			
WWUI4	▶VOL4			
WWUI5	▶VOL1	▶VOL2	▶VOL3	
WWUI6	▶VOL4			
WWUI7	▶VOL4			
WWUI8	▶VOL1	▶VOL2	▶VOL3	▶VOL4
WWUI9	▶VOL4			
WWUI10	▶VOL5	▶VOL6		

Access Rights

The creation of an identity limits the iSCSI initiators able to access an iSCSI target and its underlying volumes. Now, you want to define the access rights for each identity-target pair. When you couple an identity and target, you assign access rights: read-write (RW), read-only (RO) or not accessible (NA). The access rights are per identity-target pair. An identity can be coupled with multiple targets, each time with different access rights. As well, a target can have multiple identities, each with different access rights.

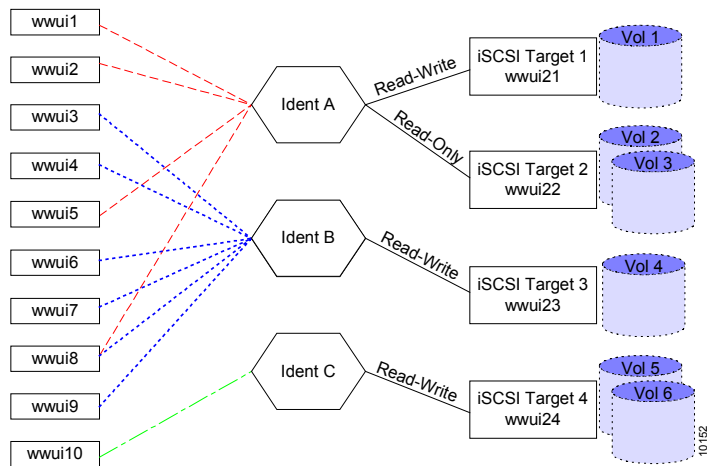


Figure 58. Access Rights per Identity-Target Pair

In Figure 58, Identity A is coupled with both Target 1 and Target 2. The Identity A - Target 1 pair is assigned iSCSI initiator read-write access to Target 1 volumes. The Identity A - Target 2 pair, however, is assigned iSCSI initiator read-only access to Target 2 volumes.

When you assign an identity to a target, you give the identity a *position*, beginning with 1 and increasing in number with increasing specificity of the identity. A position is an identity's rank in the V-Switch scan for an iSCSI initiator - identity match. When the V-Switch scans the list of identities coupled with a target, it starts with the highest position and stops with the first iSCSI initiator - identity match. The V-Switch takes the first fit; not the best fit.

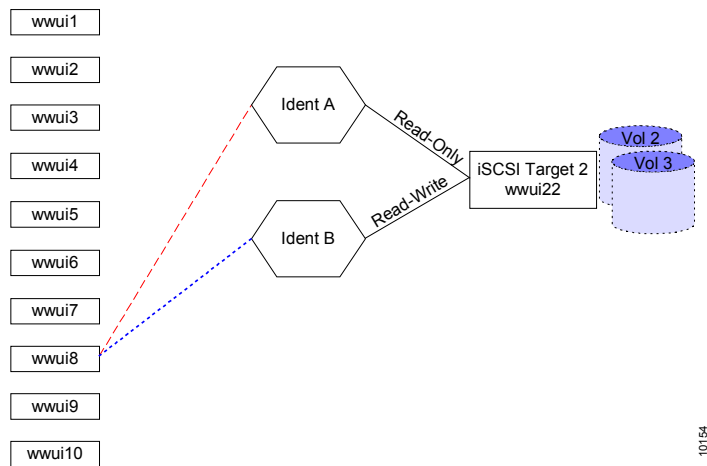


Figure 59. iSCSI Initiator in Two Different Identities

In Figure 59, iSCSI initiator WWUI8 is part of Identity A and Identity B. If Identity A and Identity B are coupled with Target 2, iSCSI initiator WWUI8 will have two different access options to Volumes 2 and 3: read-write and

read-only, depending on the positioning of the identities. If Identity A is assigned position 1 and Identity B is assigned position 2, Identity B is scanned first by the V-Switch. A match is made and the scan is stopped. No further identities will be scanned. Therefore, iSCSI initiator WWUI8 will be granted read-write access.

If the positions are reversed and Identity B is assigned position 1 and Identity A is assigned position 2, iSCSI initiator WWUI8 will be granted read-only access.

Authentication

The V-Switch supports the authentication methods CHAP and SRP for the iSCSI initiator. The credentials for CHAP and SRP are the combination of user name + password. An authentication method is assigned per identity and not per iSCSI initiator. An identity can be assigned one or both authentication methods. If no authentication method is assigned, all listed iSCSI initiators in an identity will have un-authenticated login rights.

When an iSCSI initiator logs in to a target, its WWUI is checked against the identity initiator list. After the iSCSI initiator passes the identity stage, if credentials are configured, the iSCSI initiator must authenticate itself. The credentials list is checked for the iSCSI initiator's user name + password. The list can contain a separate user name + password for each initiator; a few user name + password pairs common to a few initiators or a single user name + password for all initiators in the identity.

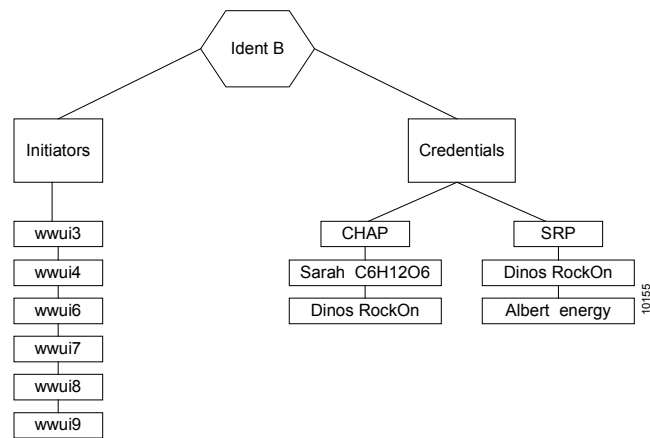


Figure 60. Identity with iSCSI Initiators and Credentials

In Figure 60, there are six iSCSI initiators in Identity B but only four user name + password credentials. Certain initiators have the same user name + password configured on them.

Default Identity

When you create a target, it is automatically coupled to a default identity. The default identity gives un-authenticated read-write access to all iSCSI

initiators. The default identity is assigned position 0, meaning it is the last scanned. Unlike user-created identities, the default identity cannot be uncoupled from a target. Its access can only be modified.

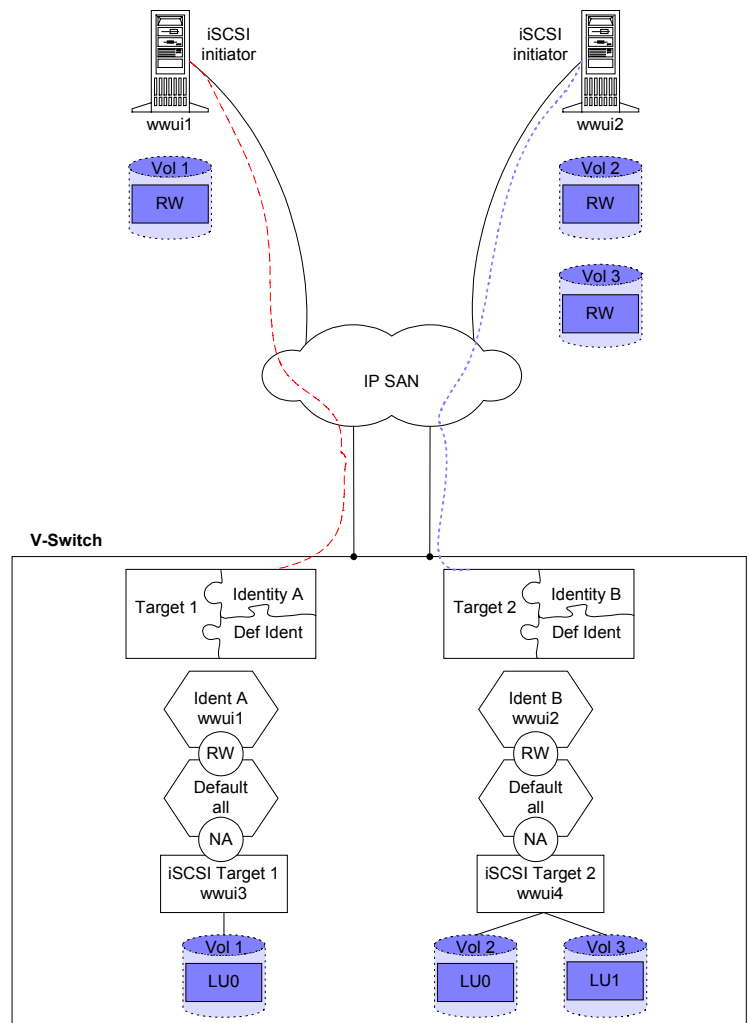


Figure 61. Modifying Default Identities

In Figure 61, the default identities for Target 1 and Target 2 have been modified to not accessible (NA) for all initiators. Remember that the default identity is in position 0 so it is the last position scanned by the V-Switch.

Target 1 is coupled with Identity A with read-write (RW) access to Identity A iSCSI initiators, meaning WWUI1.

Target 2 is coupled with Identity B with read-write (RW) access to Identity B iSCSI initiators, meaning WWUI2.

When iSCSI initiator WWUI1 logs in to Target 1, the V-Switch first scans Identity A and finds the initiator listed there. The scan stops and the initiator is granted read-write access to Target 1's underlying volume, Volume 1.

If iSCSI initiator WWUI1 tries to login to Target 2, the V-Switch first scans Identity B. It does not find the initiator listed so it continues to scan the next identity, the default identity. The default identity blocks all iSCSI initiators, including WWUI1. The scan stops and the initiator is denied access to Target 2's underlying volumes, Volume 2 and Volume 3, since the default identity is configured as not assessable.

When planning and creating identities, keep in mind that:

- Each identity can contain one or more iSCSI initiators.
- Each identity can be assigned one or both login authentication methods.
- Each identity can be attached to more than one target.
- Each target is first automatically coupled to a default read-write un-authenticated access identity.
- Each target can have more than one identity.

Creating an iSCSI Target

All CLI names and aliases are case sensitive

You can create all of your iSCSI targets using the CLI command **iscsi target create**. These targets will have no initial associated LUNs and will not be exposed to hosts when first created. It will have the default identity automatically attached to it. Later, when you want to expose volumes on the target, you can attach LUNs to the targets using the CLI command **volume expose**.

If you are working in a V-Switch cluster, each target and LUN must be configured on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see "Introduction to V-Switch Clusters," page 72.

iscsi target create

You need to define three parameters to create an iSCSI target:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	USER-ASSIGNED ALIAS FOR ISCSI TARGET	MANDATORY	finance
-tn	TARGET WWUI	USER-ASSIGNED WORLD-WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY	sanrad.billing
-device	DEVICE	ALIAS OF V-SWITCH TO EXPOSE TARGET ON	MANDATORY	VSwitch1

Example:

If you are working in a V-Switch cluster, each target must be configured on both V-Switches.

The target finance is created on V-Switch 1. The WWUI of Finance is billing.sanrad, as shown in Figure 62.

```
iscsi target create -ta finance -tn sanrad.billing -device VSwitch1
```

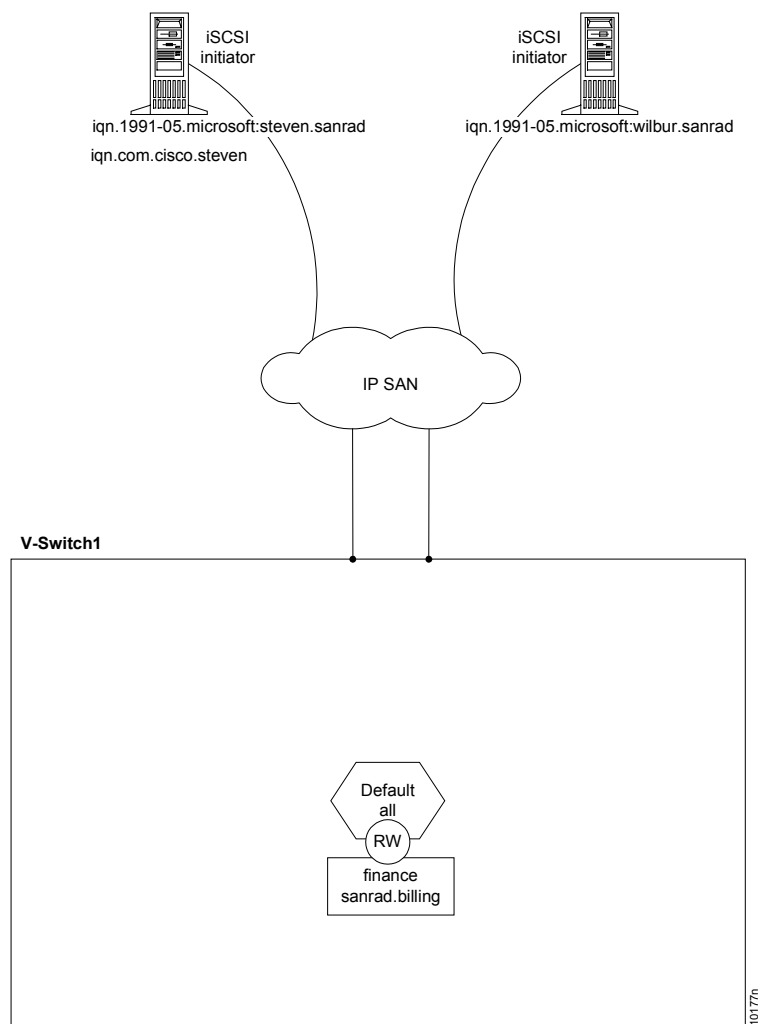


Figure 62. Creating a Target

Viewing iSCSI Targets

Use the CLI command `iscsi target show` to view all created iSCSI targets.

```
iscsi target show
```

Table 22: iSCSI Targets

Target Alias	Target Name	# of LUs	Exposed On:
finance	sanrad.billing	0	Not exposed
musicbox	musicbox.sanrad	1	VSwitch1

Viewing iSCSI Target Details

Use the CLI command `iscsi target details` to view the details of an iSCSI target.

```
iscsi target details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	USER-ASSIGNED ALIAS FOR iSCSI TARGET	MANDATORY	Finance

Table 23:

Target Alias:	nms153
Target Name:	eui.00081affff012345
CHAP User Name:	sanrad
Status:	OK
Number of Ports:	1
Port Name:	eui.00081affff012345 ,t,0
Number of LUs:	2
# Login Failures:	5
Last Failure Time:	10/12/04 15:30
Last Failure Type:	Authentication Error
Last Initiator Name:	Plony
Last Initiator IP:	1.2.3.4

Viewing Access Rights

After creating a target, use the CLI command `acl show` to view the target's automatically connected default identity.

```
acl show
```

Table 24: Default Identity Target Access

Target	Position	Identity	Access
finance	0	DEF_ALL	read-write
musicbox	0	DEF_ALL	not accessible
musicbox	1	musicdept	read-write

Changing the Default Identity

If you are working in a V-Switch cluster, the default access rights must be disabled on both V-Switches.

In the event of a failover, if the default access rights are not modified on both V-Switches, all volumes attached to the target will be read-write accessible to all iSCSI initiators.

When a target is created, a default access control identity is automatically assigned to its position 0. The default identity allows all hosts read-write access to the target and its underlying volume(s).

If you want to specify other access rights, you must change the general read-write access. Use the CLI command `acl set` to modify a target's access rights and identity position.

If you add or modify identities on a target after its volumes have been exposed, the access rights will take effect only at the next login for each iSCSI initiator. Therefore, it is recommended to modify the default access rights for a target first before creating new identities to insure that it will not inadvertently be exposed to all iSCSI initiators in the beginning.

`acl set`

You need to define four parameters to modify an identity:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-ta</code>	TARGET	ALIAS OF TARGET TO CONNECT WITH ACL IDNETITY	MANDATORY	<code>finance</code>
<code>-id</code>	IDENTITY	ACL IDENTITY	MANDATORY	<code>DEF_ALL</code>
<code>-acc</code>	ACCESS	ACCESS RIGHTS TO TARGET: DEFAULT=RW RW =READ-WRITE RO = READ-ONLY NA =NOT ACCESSIBLE	OPTIONAL	<code>na</code>
<code>-pos</code>	POSITION	IDENTITY RANK IN ACCESS RIGHT EVALUATION SCAN DEFAULT=NEXT HIGHEST AVAILABLE NUMBER	OPTIONAL	<code>0</code>

Example

The default access rights for the target `finance` are changed to not accessible meaning a non-specific host is not allowed access to the target `finance`.

```
acl set -ta finance -id def_all -acc na
```

Creating an Identity

If you are working in a V-Switch cluster, each identity must be configured on both V-Switches.

If you are working with an iSNS server, all hosts are able to see the target but only those hosts with access rights are able to connect to the target.

If you want to limit host, meaning iSCSI initiator, access to targets, you must create an identity that is more discriminate than the default identity. Use the CLI command `acl identity create` to name and describe an identity.

When creating identities, keep in mind that:

- Each identity can contain one or more iSCSI initiators.
- Each identity can be assigned one or both login authentication methods.
- Each identity can be attached to more than one target.
- Each target is first automatically coupled to a default read-write un-authenticated access identity.
- Each target can have more than one identity.

`acl identity create`

You need to define two parameters to create an identity:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-alias</code>	ALIAS	ALIAS FOR IDENTITY	MANDATORY	<code>accounting</code>
<code>-info</code>	INFORMATION	INFORMATION ON IDENTITY	OPTIONAL	<code>accountants allowed read-write access to accounting records</code>

Example

An identity, `accounting`, is created for those accountants allowed read-write access to the accounting records, as shown in Figure 63, page 121.

```
acl identity create - alias accounting - info
accountants allowed read-write access to accounting
records
```

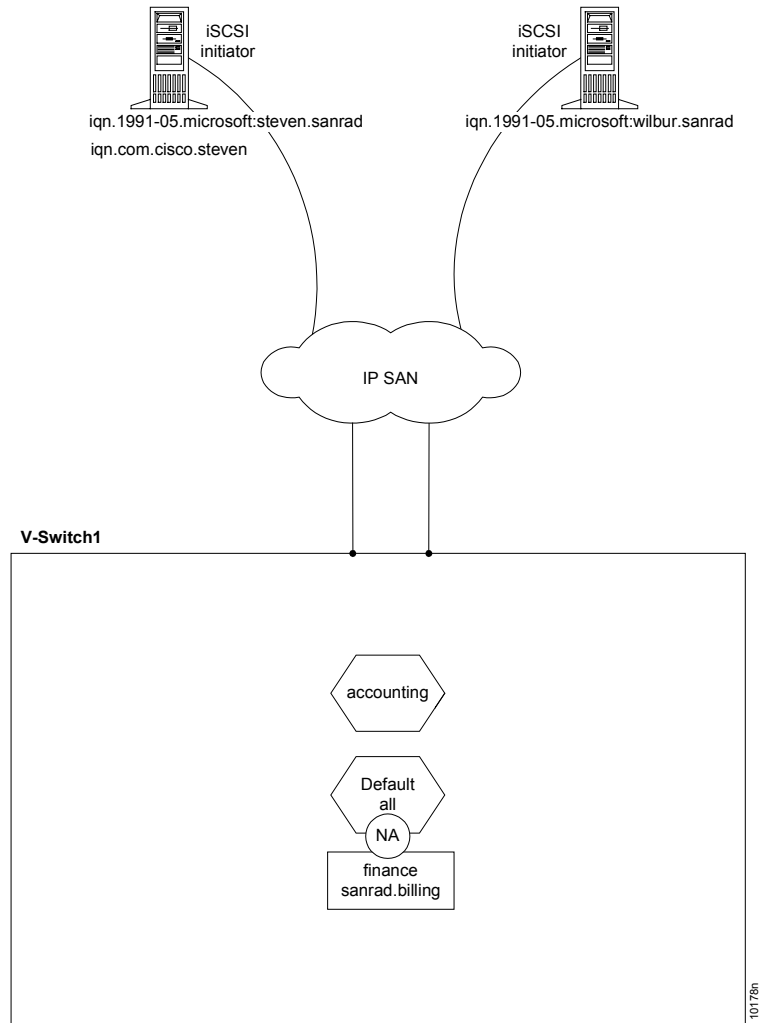


Figure 63. Creating an Identity

Adding Initiators to an Identity

If you are working in a V-Switch cluster, each initiator must be added on both V-Switches.

After creating an identity, you can begin adding hosts by their iSCSI initiator WWUIs to the identity. The identity is a group of iSCSI initiators. It is not enough for an authorized host to request access to a target. The host must be requesting access from the correct iSCSI initiator. Use the CLI command `acl identity add name` to add iSCSI initiators to an identity. Repeat this command to add all of the desired host initiators to the identity.

`acl identity add name`

You need to define two parameters to add an initiator an identity:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-id</code>	IDENTITY	ALIAS OF IDENTITY	MANDATORY	<code>accounting</code>
<code>-name</code>	INITIATOR NAME	WWUI OF INITIATOR	MANDATORY	<code>iqn.1991-05. microsoft: steven.sanrad</code>

Example

The host, steven, is added to the identity accounting according to his iSCSI initiator wwui, iqn.1991-05.microsoft:steven.sanrad.

```
acl identity add name -id accounting -name iqn. 1991-05.
microsoft: steven.sanrad
```

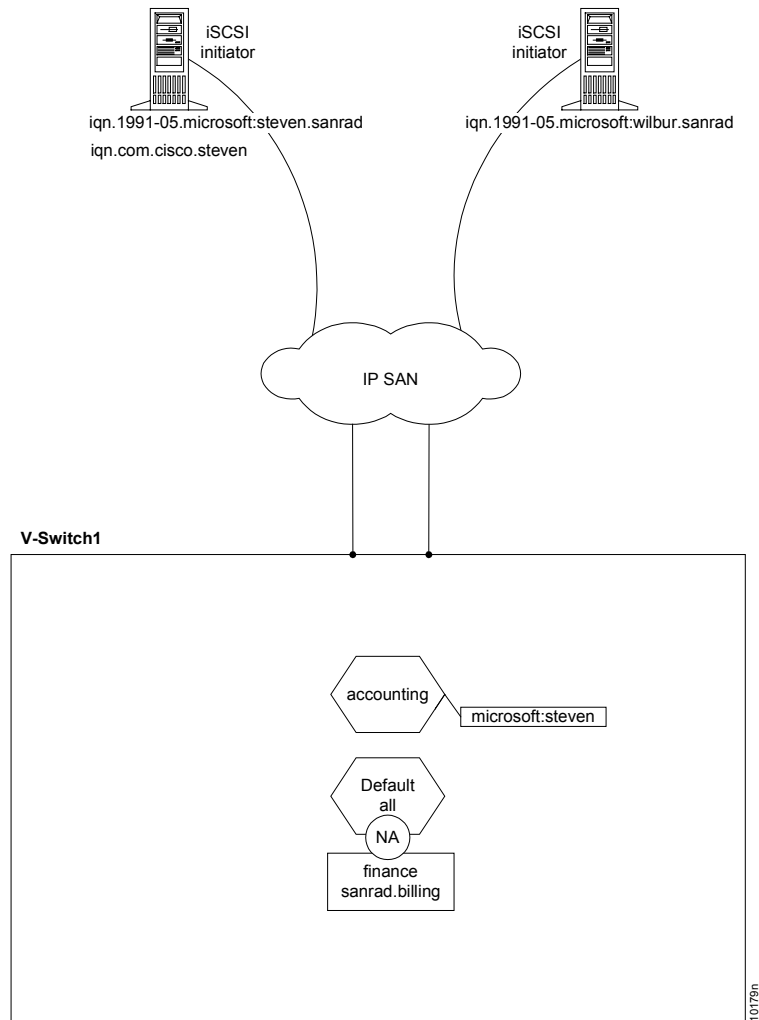


Figure 64. Adding an Initiator

If a host has more than one iSCSI initiator installed, both initiators can be included in the identity.

```
acl identity add name -id accounting -name iqn.com.cisco.steven
```

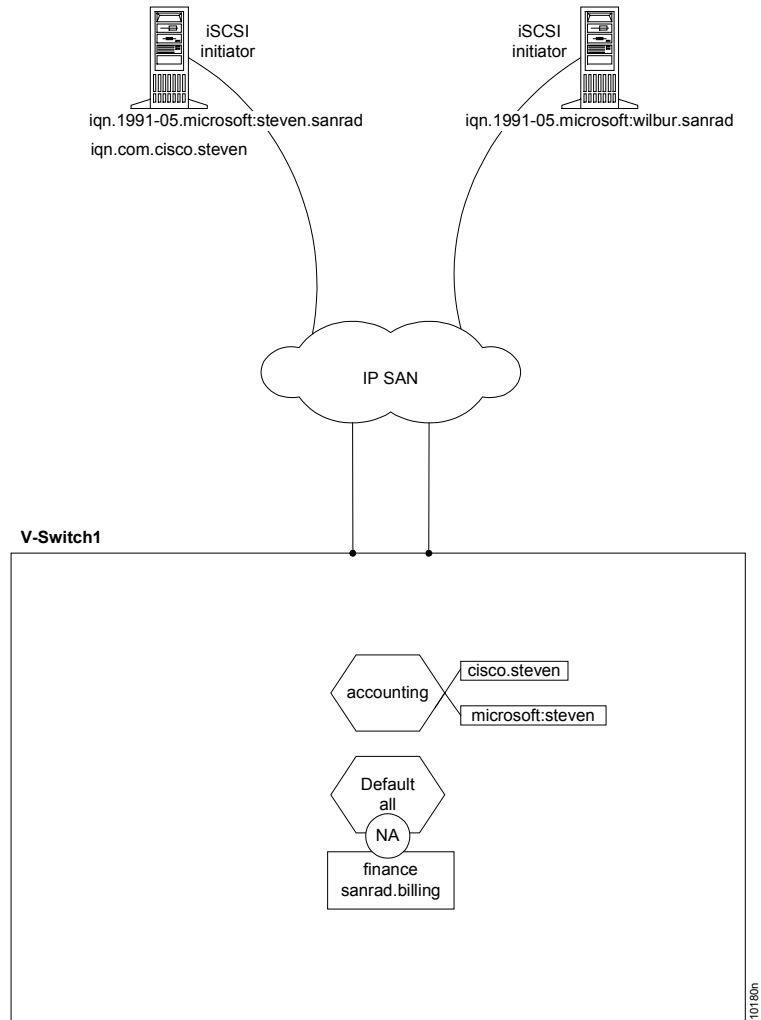


Figure 65. Adding a Second Initiator

Assigning Identity Credentials

If you are working in a V-Switch cluster, the identity authentication method(s) must be added on both V-Switches.

In the event of a failover, if each identity does not require authentication on both V-Switches, each attached identity will have free access to the target's underlying volumes.

You can require initiator authentication before allowing access to a target and its underlying volume(s). The V-Switch supports CHAP and SRP authentication methods. Microsoft and Cisco initiators support CHAP. Use the CLI command **acl identity add chap/srp** to assign a login authentication method(s) to initiators in an identity.

An assigned authentication method encrypts the host login name and password. The authentication method does not encrypt the virtual volume data transferred. The host login and password do not have to relate to the iSCSI initiator WWUI. They can be any selected character strings.

If you are working with a Microsoft initiator and configuring target authentication, note that the V-Switch exchanges the final character in the password with a zero. Therefore, do not configure initiator passwords with a zero as the final character. CHAP passwords must be between twelve to sixteen characters in length.

acl identity add chap

You need to define four parameters to assign the CHAP/SRP authentication method to an identity:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	ALIAS OF IDENTITY	MANDATORY	accounting
-us	USER NAME	INITIATOR USER NAME	MANDATORY	steven
-pw	USER PASSWORD	INITIATOR PASSWORD	MANDATORY UNLESS A RADIUS SERVER IS USED 12-16 CHAR STRING	oneveryhot dude
-radius	RADIUS	RADIUS SERVER	OPTIONAL DEFAULT: NO	No parameter required

Example

The user name, steven, with user password, oneveryhotdude, is assigned CHAP credential verification in the identity accounting.

```
acl identity add chap -id accounting -us steven -pw  
oneveryhotdude
```

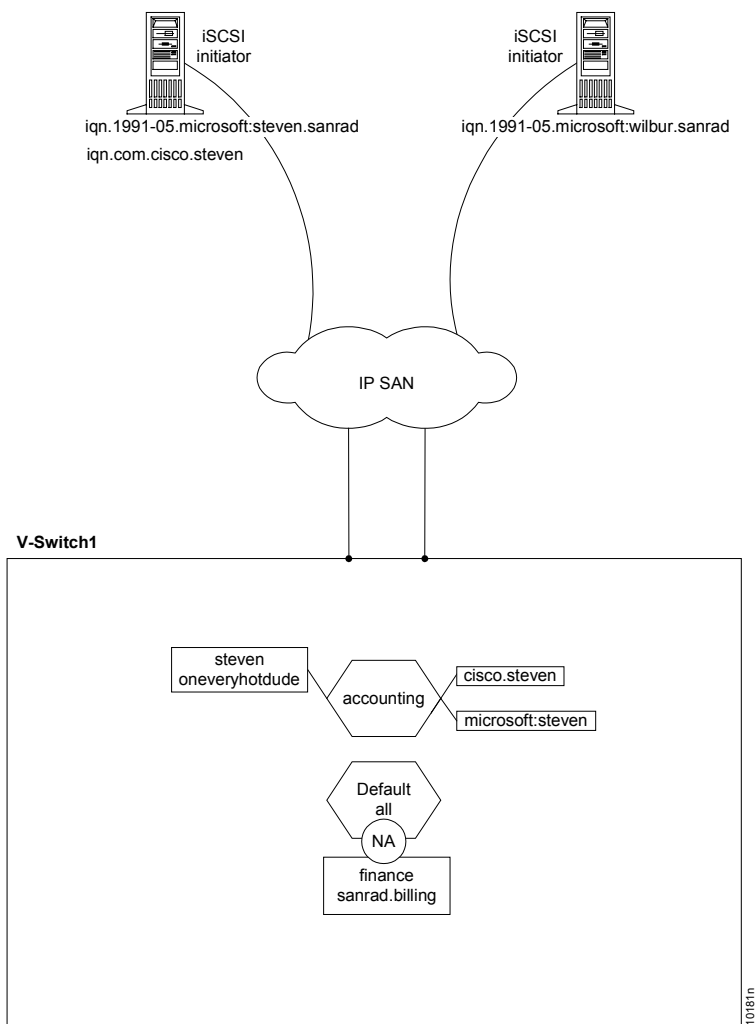


Figure 66. Assigning Credentials

If a host has more than one iSCSI initiator installed, both initiators can be included in the identity and given authentication methods. The user name and password do not need to be the same for different initiators on the same host.

```
acl identity add chap -id accounting -us steven -pw ilovecookies
```

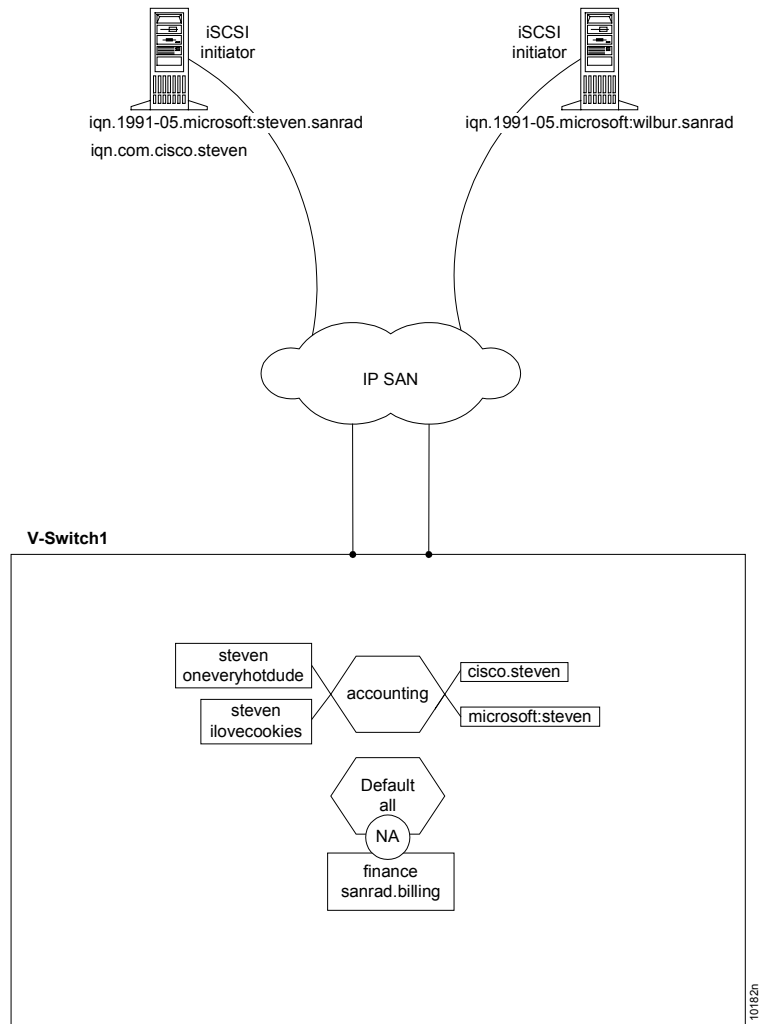


Figure 67. Adding Another Set of Credentials

After assigning iSCSI initiators and assigning credentials to an identity, use the CLI command `acl identity details` to view the list of iSCSI initiators.

`acl identity details`

You need to define one parameter to view an identity's details:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-id</code>	IDENTITY	NAME OF ACL	MANDATORY	<code>accounting</code>

```
acl identity details -id accounting
```

Table 25: Identity Details

Description:	Accounts allowed read-write access to accounting records
Initiators:	<code>iqn.1991-05.microsoft:steven.sanrad</code> <code>iqn.com.cisco.steven</code>
Credentials:	CHAP

Using a RADIUS Server

If you are working in a V-Switch cluster, the RADIUS server must be configured on both V Switches.

When CHAP user names and passwords are configured on the network in a remote RADIUS server, use the CLI command `acl identity add chap` to direct a CHAP challenge to the RADIUS server and eliminate the need to configure all user name + password pairs on the V-Switch. This decreases configuration time and increase overall network security. Use the CLI command `ip radius add` to add a RADIUS server address to the V-Switch RADIUS client.

In Figure 68, page 129, a CHAP authentication challenge is sent to the V-Switch. The V-Switch first checks if the user name is set for RADIUS authentication. If it is, the CHAP challenge is passed on to the RADIUS server. If it is not, the user name and password are compared against the pairs configured in the V-Switch.

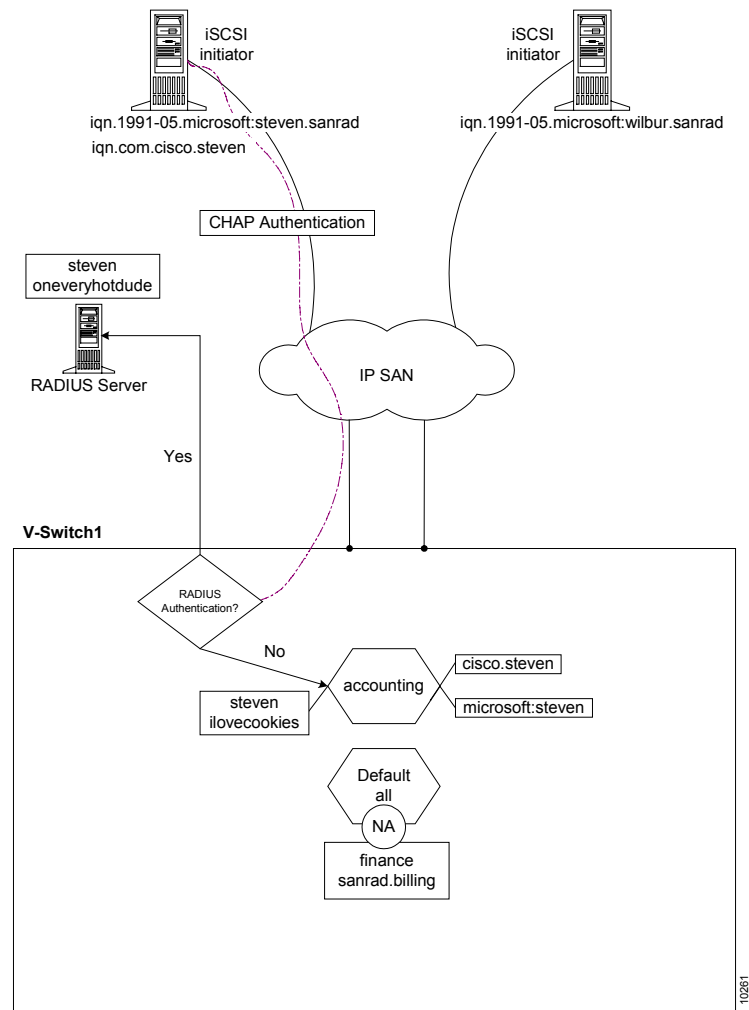


Figure 68. Sending a CHAP Authentication Challenge

`ip radius add`

You need to define three parameters to add a RADIUS server IP to the RADIUS client

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF RADIUS SERVER	MANDATORY	212.199.43.2
-p	PORT	UDP PORT	OPTIONAL	1812
-k	KEY	SHARED SECRET BETWEEN RADIUS SERVER AND V-SWITCH	MANDATORY	DataTurnsMeOn

Example:

In Figure 69, the V-Switch is configured to relay CHAP challenges to the identity, accounting, from the user, steven, to the RADIUS server. The V-Switch is configured to communicate with the RADIUS server through port 1812 to IP address 212.199.43.2. The V-Switch - RADIUS key is DataTurnsMeOn.

The user password is not configured on the V-Switch. The RADIUS server authenticates the user password and sends the results back to the V-Switch.

```
acl identity add_chap -id accounting -user steven -  
radius yes
```

```
ip radius add -ip 212.199.43.2 -p 1812 -k DataTurnsMeOn
```

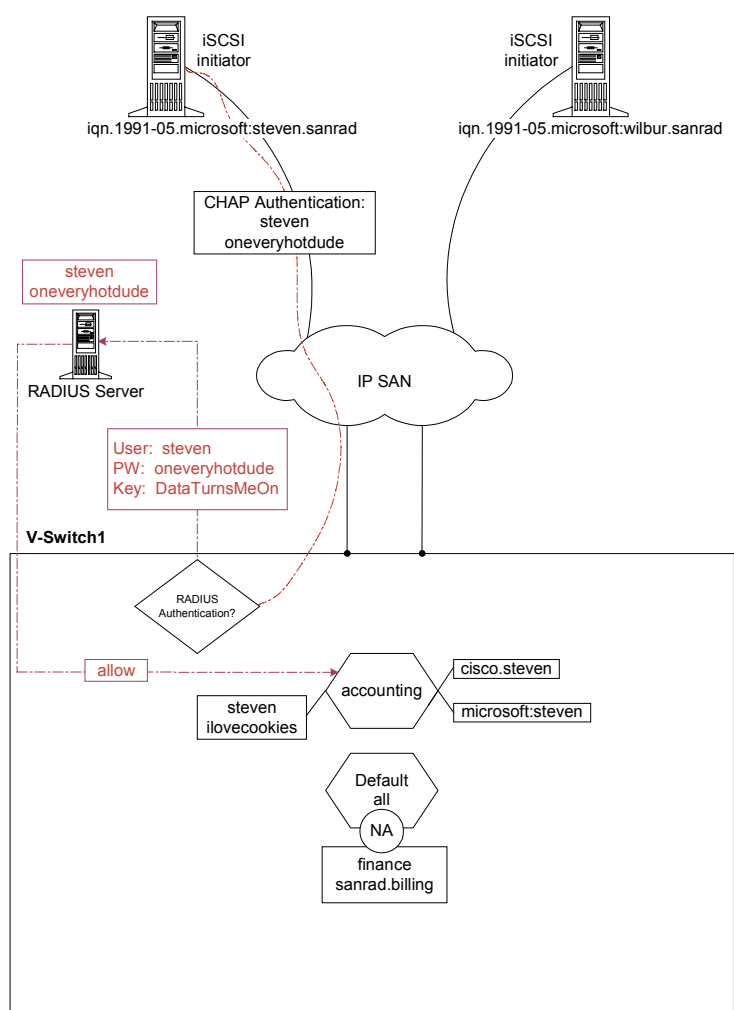


Figure 69. Logging in to a RADIUS Server

Viewing Configured RADIUS Servers

Use the CLI command `ip radius show` to view all configured RADIUS server IP addresses.

```
ip radius show
```

Table 26: Configured RADIUS IP Addresses

Address	Port
212.199.43.2	1812
212.199.56.134	1812

Connecting an Identity and Target

If you are working in a V-Switch cluster, each Identity must be connected to the target(s) on both V-Switches.

Once created, an identity must be connected to a target to provide it with access control. An identity specifies which access rights the iSCSI initiators within the Identity have to the target.

When an identity is connected to a target, it is also given a *position*. The position of the identity determines its place in the V-Switch access rights evaluation. An identity with the position 0 (default identity) is the last identity evaluated when an initiator tries to access a volume. If the initiator meets the profile of the identity, it is granted that identity's access rights. If not, the V-Switch continues to position 1. The V-Switch does not scan all identities to determine which most specifically fits the host. Therefore, identities must be positioned in decreasing specificity to function correctly. The V-Switch scans for the first fit and not the best fit.

All CLI names and aliases are case sensitive

An identity can be connected to more than one target to provide the same conditions for each target. Use the CLI command **acl add** to connect an identity to a target.

acl add

You need to define four parameters to connect an identity to a target:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF TARGET TO ATTACH TO	MANDATORY	finance
-id	IDENTITY	NAME OF ACL IDENTITY	MANDATORY	accounting
-acc	ACCESS	ACCESS RIGHTS TO TARGET: DEFAULT=RW RW =READ-WRITE RO = READ-ONLY NA =NOT ACCESSIBLE	OPTIONAL DEFAULT=RW	rw
-pos	POSITION	ACL RANK IN ACCESS RIGHT EVALUATION SCAN	OPTIONAL ASSIGNED LAST POSITION IF NOT SPECIFIED	1

Example

The identity, *accounting*, is connected to the target *finance*. *Accounting* is the second identity scanned for an initiator match. Any initiator in the *accounting* identity is given read-only access. Later, an administrator identity can be created with read-write access and placed in position 0.

```
acl add -ta finance -id accounting -acc rw -pos 1
```

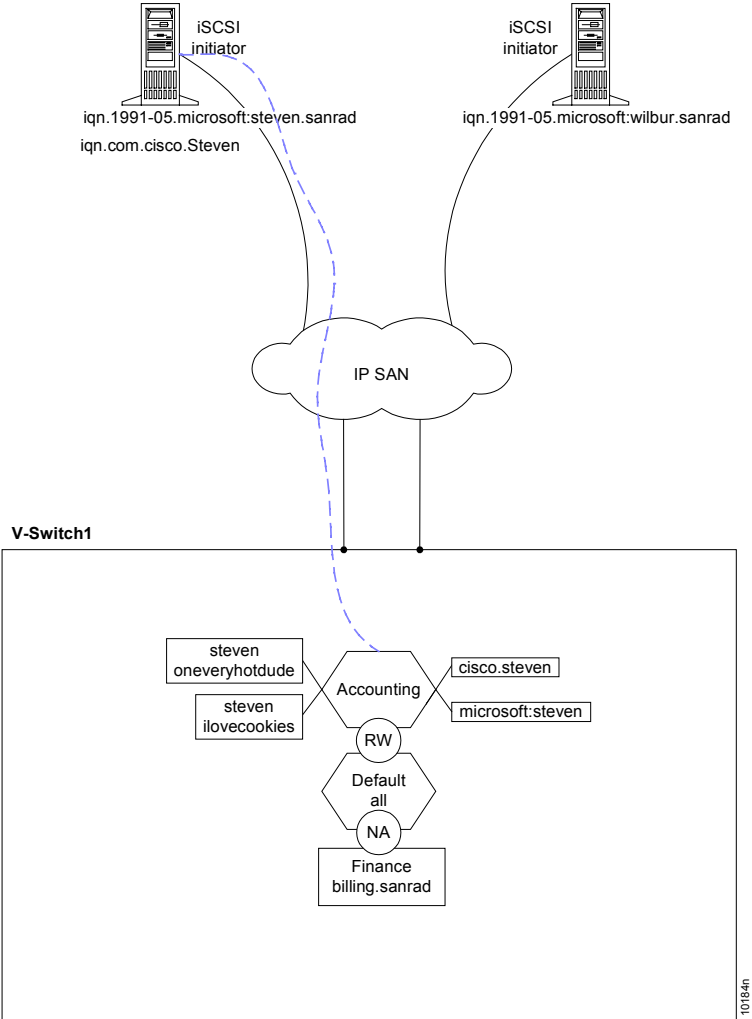


Figure 70. Connecting a Target and Identity

Exposing an iSCSI Target and LUN

The first LUN assigned to an iSCSI target must be LU 0.

A LUN value cannot be larger than 255.

All CLI names and aliases are case sensitive.

A snapshot volume must be exposed on the same V-Switch as the source volume.

To make a volume accessible to a host, you need to assign a LUN to it, attach the LUN to an iSCSI target and expose the target. The CLI command **volume expose** is used in two ways:

- Create and expose a new target.
- Expose an existing target.

The CLI command **volume expose -new** creates a new iSCSI target, assigns a volume LUN and then exposes the new target.

After creating a target and LU0, you can add additional LUNs to the target using the CLI command **volume expose** (without the **-new** switch).

volume expose

If you are working in a V-Switch cluster, each target and LUN must be configured on both V-Switches in the V-Switch cluster. For more information on V-Switch clusters, see “Introduction to V-Switch Clusters,” page 72.

If you add or modify identities on a target after its volumes have been exposed, the access rights will take effect only at the next login for each iSCSI initiator.

You need to define six parameters to create and expose an iSCSI target and volume LUN:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-new	NEW TARGET	NEW iSCSI TARGET TO CREATE	OPTIONAL	No parameter required
-vol	VOLUME ALIAS	ALIAS OF VOLUME TO CREATE LU0 AND TARGET FOR	MANDATORY	Vol1
-ta	TARGET ALIAS	USER-ASSIGNED ALIAS OF TARGET TO CREATE	MANDATORY	finance
-lun	LU NUMBER	USER-ASSIGNED LUN FOR EXPOSING VOLUME	MANDATORY ON EXISTING TARGET	0
-tn	TARGET WWUI	USER-ASSIGNED WORLD WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY ON A NEW TARGET	sanrad.billing

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-device	DEVICE	ALIAS OF V-SWITCH TO EXPOSE TARGET ON	MANDATORY ON A NEW TARGET	VSwitch1

Example 1:

The target finance already exists. The WWUI of finance has already been assigned to the target. The volume Vol1 is assigned LU0 and attached to the target finance. The exposing device is VSwitch1.

```
volume expose -vol Vol1 -ta finance -lun 0
```

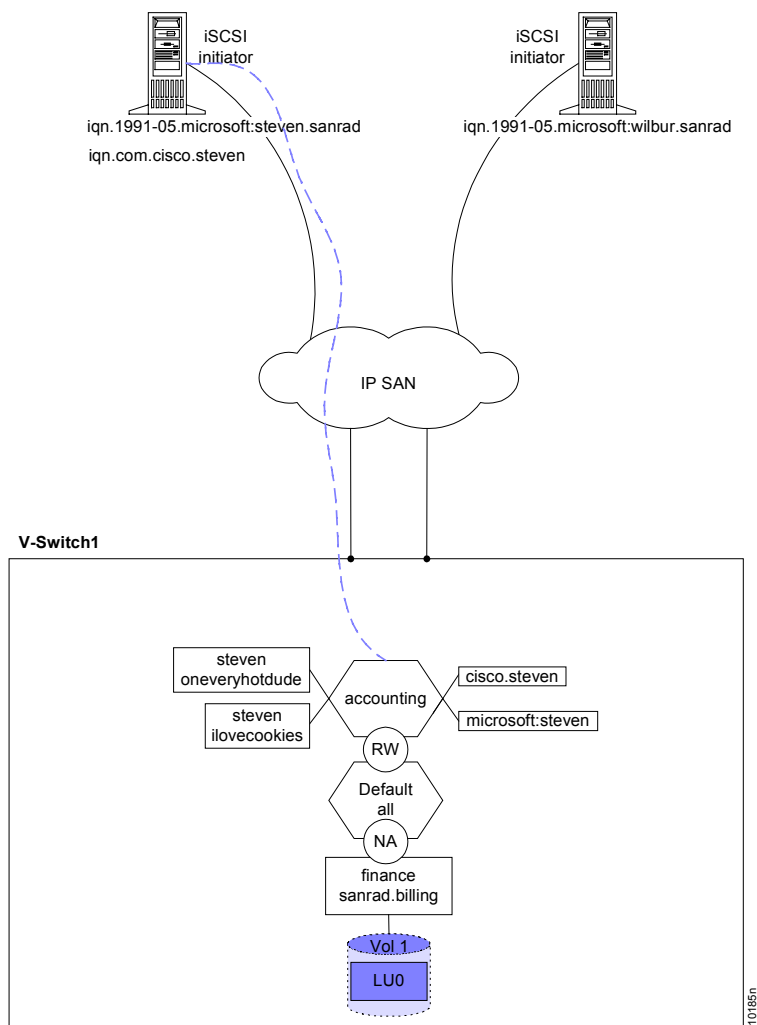


Figure 71. Exposing a Volume

Example 2:

If you are working in a V-Switch cluster, this target and LUN must be configured on both V-Switches.

The target musicbox is created. The WWUI of musicbox is sanrad.musicbox. The volume Concat1 is automatically assigned LU0 and attached to the target musicbox on VSwitch1.

```
volume expose -new -vol Concat1 -ta musicbox -tn
sanrad.musicbox -device VSwitch1
```

Viewing LUNs

You can view all created LUNs using the CLI command `lu show`.

```
lu show
```

Table 27: Details of all LUNs

LUN	Tgt Alias	Volume	Oper Status
0	pilote	Stripe1	Active
0	spirou	Concat2	Active
1	pilote	Mir1	Active
0	lucky	Mirror/Concat	Active



Advanced Volume Operations

IN THIS CHAPTER

Once you have configured your initial basic volume topology, you can do more advanced volume operations.

INTRODUCTION TO
ADVANCED VOLUME
CONFIGURATIONS

COPYING A VOLUME
(OFF-LINE COPY)

SYNCHRONIZING A
VOLUME

ADDING A CHILD TO A
MIRROR (ON-LINE
COPY)

CREATING A
SNAPSHOT

BREAKING A MIRROR

RESIZING A VOLUME

EXPANDING A VOLUME

This chapter explains how to:

- ❑ Create an off-line volume copy.
- ❑ Create an on-line volume copy.
- ❑ Break a mirror to remove a child.
- ❑ Create a snapshot.
- ❑ Increase a volume's capacity.

Introduction to Advanced Volume Configurations

The V-Switch supports several advanced volume operations. Some do the same or similar functions. Each has its own advantages so it is important to understand their differences to best choose the function most appropriate for you SAN.

Data Replication: Off-line versus On-line

Off-line data replication creates a copy of a volume. The source volume can be any type of volume. If the source volume is exposed, it must be taken offline, creating an interruption of service to the host. The destination volume must also be off-line. On-line data replication is done via a mirrored volume. The source and destination volumes must be children the same mirror. On-line data replication presents no interruption of service. Because on-line replication must take into account the possibility of read/write operations to the source volume during the data replication, it is slower than off-line data replication.

Mirror versus Snapshot

A mirrored volume copy is a full, complete volume copy. A snapshot is only a record of changes to a volume. Because of this, its capacity can be smaller than a mirrored volume copy by as much as eighty percent. Both a mirrored volume copy and a snapshot can be exposed to a host like any other volume. However, unlike a mirrored copy, a snapshot is nonfunctional if its source volume goes off-line or its capacity is exceeded in write operations. A snapshot volume must also be exposed on the same V-Switch as its source volume while a mirrored copy has no dependency on its source.

Actual Capacity versus Potential Capacity

Potential capacity is the maximum capacity a volume could be. Actual capacity is the capacity that the server recognizes a virtual volume as having.

Resizing versus Expanding

Resizing increases a virtual volume's potential capacity. Expanding increases a virtual volume's actual capacity. A volume must first be resized. Only after a volume is resized can it be expanded.

Copying a Volume (Off-line Copy)

Data from any volume type can be replicated offline using the CLI command `volume copy create`. Off-line replication is faster than on-line replication but both the source and destination volumes must be off-line which can create an interruption of service to the volume host(s). Because snapshot volumes are internal (off-line) volumes, this is a way of copying a snapshot volume.

```
volume copy create
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-src</code>	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	<code>ScienceLab</code>
<code>-dst</code>	DESTINATION	ALIAS OF VOLUME TO COPY TO	MANDATORY	<code>ScienceLabII</code>

```
volume copy create -src ScienceLab -dst ScienceLabII
```

Synchronizing a Volume

If one child of a mirrored volume, the source, already contains data, the data can be replicated to the second child, the destination, using the CLI command `volume mirror sync`. This can be done on-line while the source volume is still exposed or off-line while both the source and destination volumes are unexposed. See how to expose volumes “Volume Exposure & Security,” page 107. On-line data replication is slower but allows the source volume to remain on-line with no interruption of service to the volume host(s). Off-line replication is faster than on-line replication but both the source and destination volumes must be taken off-line which can create an interruption of service to the volume host(s).

See the working example of off-line data replication “Replicating Data Off-line,” page 264.

```
volume mirror sync
```

You need to define two parameters to synchronize a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-src</code>	SOURCE VOLUME	ORIGINAL VOLUME TO SYNCHRONIZE TO	MANDATORY	<code>Simple3</code>
<code>-dst</code>	DESTINATION VOLUME	NEW VOLUME TO ADD TO SYNCHRONINZE	MANDATORY	<code>Simple5</code>

Example:

The on-line volume `Simple3` is synchronized to the on-line volume `Simple5`.

```
volume mirror sync -src Simple3 -dst Simple5
```

Adding a Child to a Mirror (On-line Copy)

If you are working in a V-Switch cluster, the child must be added on both V-Switches.

To perform on-line data replication, either by increasing the number of children in a mirrored volume or creating a mirrored copy of any other type of volume, except transparent and snapshot volumes, you can use the CLI command `volume mirror add`.

Since this is on-line data replication, the source volume does not need to be taken off-line and write operations to the source volume can continue while the mirror is being created. Any data written to the volume will be included in the added child(ren). Use this command to replace a failed disk in a mirrored volume without taking the mirror off-line.

The added child can be any type of volume, except transparent or snapshot, and it must be the same size or greater than the actual capacity of the mirror volume.

In Figure 72, a mirrored volume with two children has another child added. The mirrored volume stays at the head of the hierarchy.

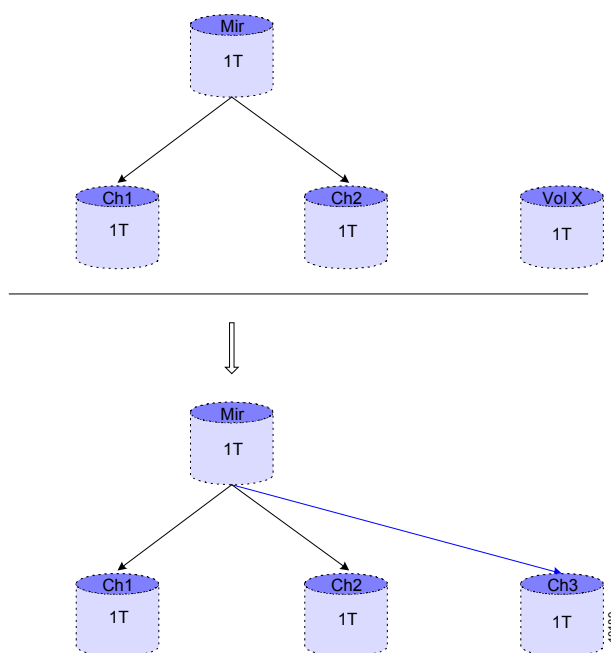


Figure 72. Adding Another Child to a Mirror

In Figure 73, page 142, a concatenated volume becomes one child of a new mirrored volume. This adds a level to the hierarchy. The new mirrored volume becomes the head of the volume hierarchy. The new mirrored volume automatically assumes the LUN from the concatenated volume.

For more information on attaching volumes to LUNs, “Exposing an iSCSI Target and LUN,” page 134.

Creating a mirror from a single volume creates data redundancy. Adding an extra child to a mirror does not create data redundancy. It increases the existing redundancy.

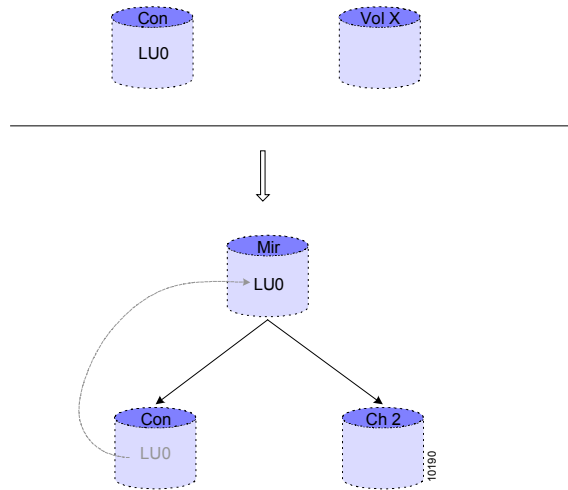


Figure 73. Creating a Mirror to Add Data Redundancy

`volume mirror add`

You need to define four parameters to add a mirrored volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME	SOURCE VOLUME TO ADD MIRROR TO	MANDATORY	Mirror5
<code>-ch</code>	CHILD	NEW CHILD TO ADD TO MIRROR	MANDATORY	Simple10
<code>-no sync</code>	NO SYNCHRONIZATION	DISABLE AUTOMATIC MIRROR SYNC	OPTIONAL NO SYNC IF USED	No parameter required

Example:

In Figure 74, the simple volume, Sim6, is added as the third child to mirrored volume Mir4.

```
volume mirror add -vol Mir4 -ch Sim6
```

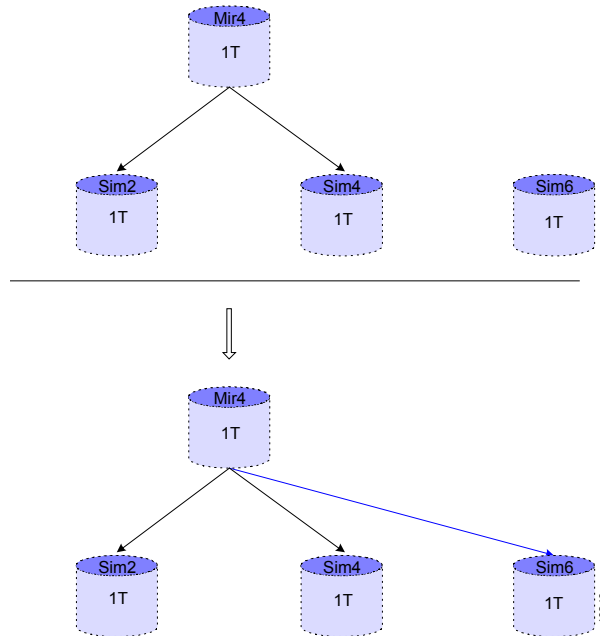


Figure 74. Adding Sim6 to Mir4

Use the CLI command `volume mirror show` to view the status of all mirror synchronizations.

```
volume mirror show
```

Source	Destination	Oper Status	Admin Status	Progress
Sim4	Sim6	Operating	Synchroniz e	60%
Ch1	Ch3	Ended OK	Dummy	100%
Simple10	Simple12	Ended error	Abort	-

Creating a Snapshot

You can create a *snapshot*, a point-in-time copy, of any volume at the top of a hierarchy using the CLI command `volume create snapshot`. A snapshot does not create a full copy of its source volume. It is a dynamic and dependent volume that stores the original data from a source volume when changes to the source volume are made after the snapshot's creation. Snapshot volumes use the *copy old on write* method, copying the old source data to the snapshot and only then writing new data to the source volume.

Snapshots can be used for serverless backup, reducing the load on the application server. The backup copy from a snapshot is a full copy of the source volume at the time of the snapshot and adequate size must be allocated for the backup volume. A snapshot can be built on any volume hierarchy but, once created, cannot be used as a child in another volume hierarchy. This means that a snapshot can be created on a mirror volume with two children. However, after the snapshot is created, a mirror volume cannot be created, using the snapshot as one of the children, to copy the snapshot volume.

Figure 75, shows a source volume with its snapshot when the snapshot is first created. Initially, a snapshot is empty because there has not yet been a change in its source volume. Only when a write operation is performed on the source volume will the snapshot begin to fill up.

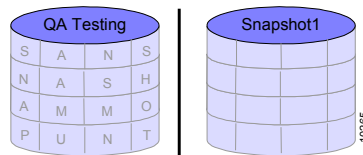


Figure 75. 1st Snapshot Created

Figure 76, page 145 shows the same source and snapshot volume after a write operation to sector 1. The snapshot records the original data from sector 1, S, to the snapshot and then the new data, B, is written to the source volume.

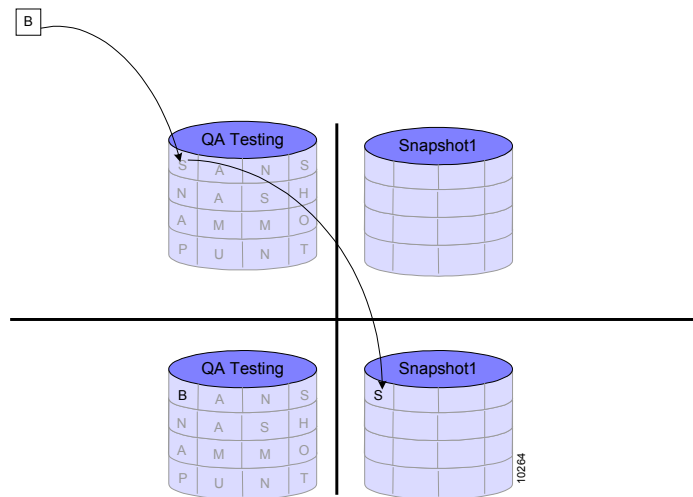


Figure 76. 1st Write to Source and Update to 1st Snapshot

The more active the write operations are to a source volume, the more capacity its snapshots need to have. SANRAD requires a beginning snapshot volume of at least one percent of the size of its source volume. A snapshot volume can be resized to accommodate a growing capacity need. A snapshot volume has a user-defined *load threshold* to monitor when a snapshot approaches full capacity. When the load threshold is exceeded, an alert is sent to resize the volume. See “Resizing a Volume,” page 153.

A snapshot volume contains a table of pointers detailing which volume to read from, the source or the snapshot, for each sector. For this reason, the full capacity of a snapshot volume is not available for source copying. The table size is:

$$\text{(Size of Source Volume in blocks)} / [(256)(\text{Size of a Block in Snapshot}/4)]$$

Deleting a snapshot volume has no effect on other snapshot volumes of the same source.

A snapshot can have read-write or read-only access and, when exposed, it must be exposed on the same V-Switch as its source volume.

volume create snapshot

You need four parameters to create a snapshot volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	SNAPSHOT NAME	MANDATORY	
-src	SOURCE	SOURCE OF SNAPSHOT	MANDATORY	
-ch	CHILD	SNAPSHOT CHILD	MANDATORY	
-lt	LOAD THRESHOLD	PERCENTAGE FULL AT DESTINATION TO TRIGGER AN ALARM	OPTIONAL DEFAULT: 80%	

Example:

Figure 77 shows a source volume with its first snapshot when the snapshot is first created. Initially, a snapshot is empty because there has not yet been a change in its source volume. Only when a write operation is performed on the source volume will the snapshot begin to fill up. The pointer table for the snapshot would point to the source volume for all sectors.

```
volume create snapshot -vol Snapshot1 -src QATesting -dst Snapshot1 -lt 80
```

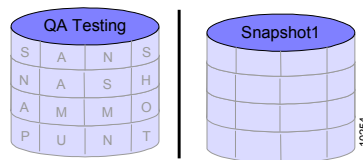


Figure 77. 1st Snapshot

Figure 78, page 147 shows the same source and snapshot volume after a write operation to sector 1. The original data, S, from sector 1 is first copied to the snapshot and then the new data, B, is written to the source volume.

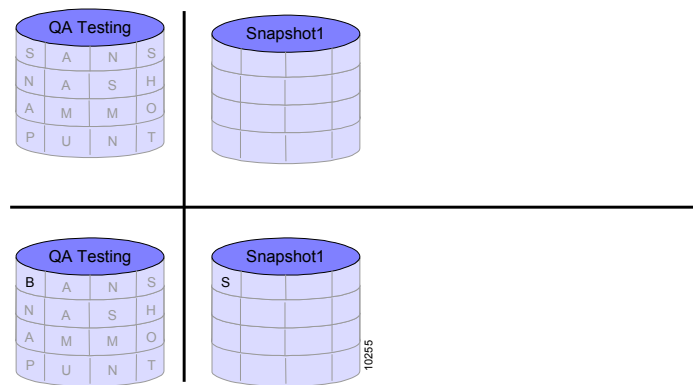


Figure 78. Update to 1st Snapshot & 1st Write to Source

Figure 79, page 148 shows the creation of a second snapshot and a second write operation to the source volume. The original data, N, A and P, from sectors 5, 9 and 13 are first copied to the Snapshot 1 & 2 and then the new data, B, E and B, are written to the source volume.

Because snapshot volumes are independent of each other, the original data must be written to each relevant snapshot, as in Snapshot 1 and 2. The pointer table is only between a single snapshot and its source; never to parts of other snapshots. Therefore, if one snapshot volume fails, no other snapshot is affected.

```
volume create snapshot -vol Snapshot2 -src QATesting -ch
Snapshot2 -lt 80
```

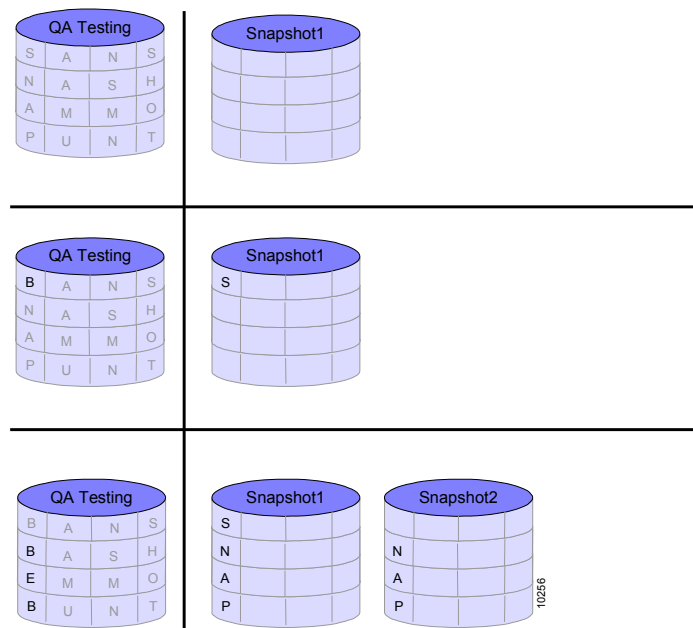


Figure 79. 2nd Snapshot Created, Update to 1st Snapshot & 2nd Snapshot and Write to Source

Figure 80, page 149, shows the creation of a third snapshot and a third write operation to the source volume. The original data, S, H, O and T, from sectors 4, 8, 12 and 16 are first copied to the Snapshot 1, 2 and 3 and then the new data, D, S, A and S, are written to the source volume.

```
volume create snapshot -vol Snapshot3 -src QATesting -ch
Snapshot3 -lt 80
```

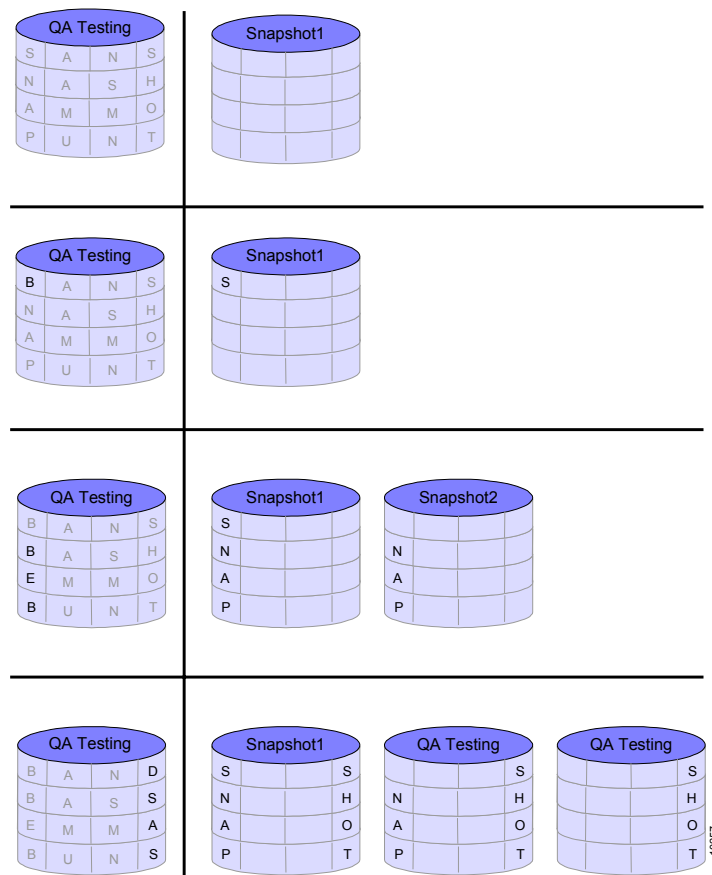


Figure 80. 3rd Snapshot Created, Update to 1st & 2nd Snapshot and Write to Source

Viewing Snapshot Volumes

You can view all created snapshot volumes using the CLI command `volume snapshot show`. Use this command to view the source and snapshot volumes, the time the snapshot was created and the percent capacity utilization. At user-defined load threshold utilization, an alert to resize the snapshot is sent.

```
volume snapshot show
```

Table 27: All Snapshot Volumes

Source	Snapshot	Date & Time	Utilization
Mirror3	Snp1Mir3	12/12/02 13:00:00	80%
Mirror3	Snp2Mir3	12/12/02 14:00:00	60%

You can view all snapshots of a single source volume using the CLI command `volume snapshot list`.

```
volume snapshot list
```

You need one parameter to view a volume's snapshots:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME	SNAPSHOT SOURCE VOLUME	MANDATORY	Mirror7

Example:

Table 28 lists the only snapshot for Mirror7.

```
volume snapshot list -vol Mirror7
```

Table 28: All Snapshots of a Specific Volume

Snapshot	Date & Time	Utilization
Snp1Mir1	12/12/02 20:00:00	20%

Breaking a Mirror

If you are working in a V-Switch cluster, the child must be removed on both V-Switches.

You can remove one of multiple children from a mirror or break a two-child mirrored volume to enable one or both of the children to be used independently. The removed child is a fully functional volume and can be exposed to any host. In particular, the removed child can be used for testing, online server-free backup or online data migration.

If you break a mirrored volume that is attached to a LUN, the remaining volume retains the attached LUN. Write operations to the source volume can continue while the mirror is being broken or a child removed but the removed child's data cannot be guaranteed to mirror the source volume. Therefore, all write operations should be suspended appropriately before breaking a mirror.

A mirror cannot be broken or a child removed if one of the volumes needs to be synchronized or it is in the process of synchronizing or copying.

In Figure 81, page 151, a child is removed from a mirrored volume with three children. If the mirrored volume is exposed, it remains functional as a mirrored volume and all read-write operations are executed.

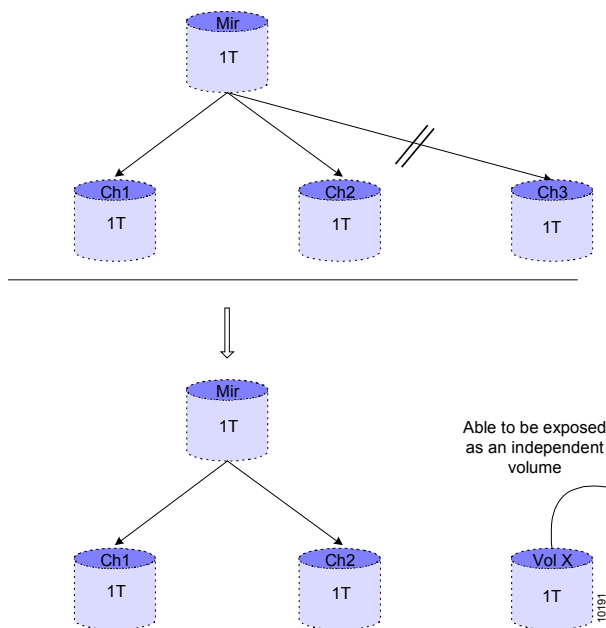


Figure 81. Removing a Child from a Mirror

In Figure 82, a child is removed from a mirrored volume with two children. This breaks the mirror. If the mirrored volume is exposed or attached to a LUN, the source volume retains the LUN. There is no need to reassign a LUN to the remaining source volume. All read-write operations will be executed without a break in service.

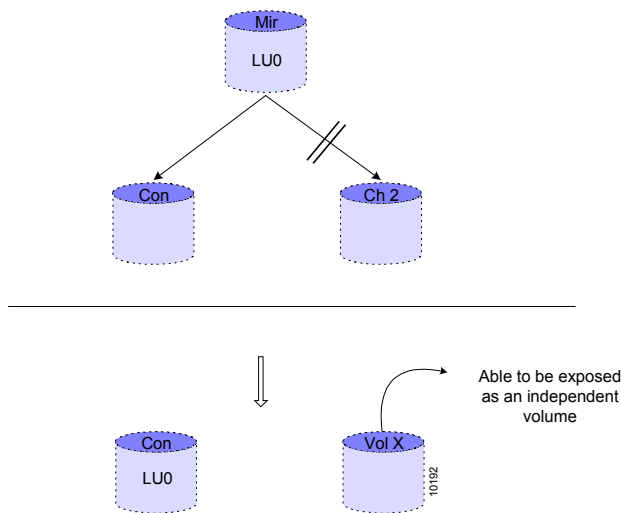


Figure 82. Breaking a Mirror

volume mirror break

You need to define two parameters to break a mirror:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME MIRROR IS ADDING TO	MANDATORY	Mirror5
-ch	CHILD	CHILD TO BREAK FROM MIRROR	MANDATORY	Simple10

Example:

In Figure 83, the simple volume Sim5 is removed from mirrored volume Mir1.

```
volume mirror break -vol Mir1 -ch Sim5
```

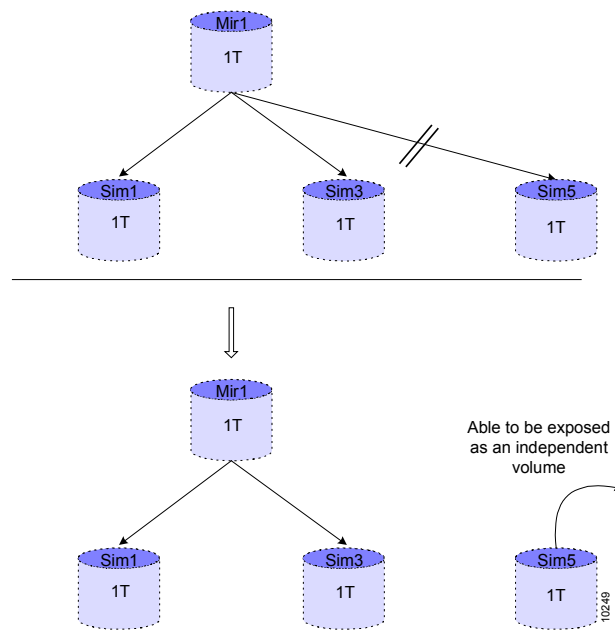


Figure 83. Removing Sim5 from Mir1

Resizing a Volume

If you are working in a V-Switch cluster, a volume must be resized on both V Switches.

You can increase a virtual volume's *potential capacity* using the CLI command `volume resize`. This is the first step in increasing a virtual volume's *actual capacity*. Potential capacity is the maximum capacity a volume could be. Actual capacity is the capacity that the server recognizes a virtual volume as having.

Resizing a volume is done while the top-level volume in the hierarchy is exposed on an iSCSI target. Simple, snapshot, concatenated and previously resized volumes can be resized. Resizing a volume concatenates a new volume with the source volume. Only a simple volume can be used to resize a simple or snapshot volume.

After one or more volumes in a hierarchy are resized, the volume must be expanded to make its actual capacity equal to its new potential capacity. See "Expanding a Volume," page 158.

In Figure 84, is a mirrored volume with a potential capacity of one terabyte. The smallest child of the mirrored volume determines the mirrored volume's potential capacity. Resizing the one-terabyte child to two terabytes will increase the mirrored volume's potential capacity to two terabytes. The actual capacity of the mirrored volume remains unchanged until it is expanded to match its potential size.

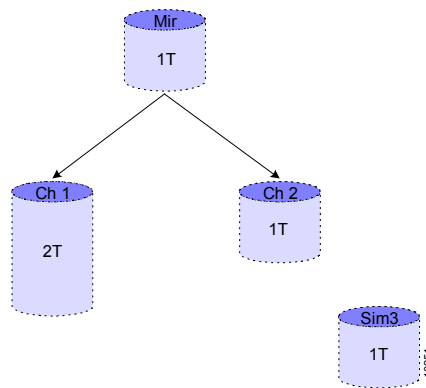


Figure 84. Asymmetrical Mirrored Volume

When a simple or snapshot volume is resized with another simple volume, the first step in their resize concatenation is the creation of a *cube*. A cube is a special type of volume intermediary created for resizing a volume through concatenation. In Figure 85, page 154, the original connection to the child to resize is broken and transferred to the cube. A cube's default alias is X+resized volume's alias. In Figure 85, page 154, the alias of the volume to resize is Ch2; the alias of the cube is XCh2.

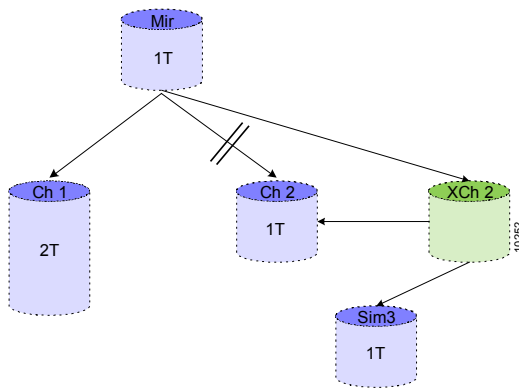


Figure 85. Creating a Cube

In Figure 86, Sim2 and Sim3 have been concatenated under the cube to a potential volume of two terabytes.

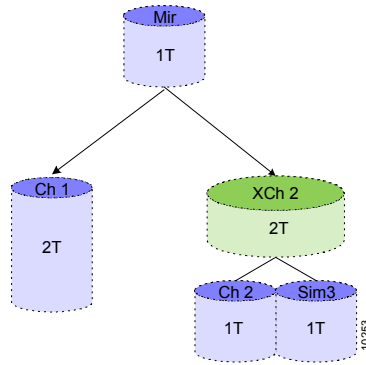


Figure 86. Resized Volume

Only one cube is created per resized simple or snapshot volume. Any further simple volumes are added to the existing cube. In Figure 87, page 155 a second one-terabyte simple volume is added to the existing cube created to resize Sim2.

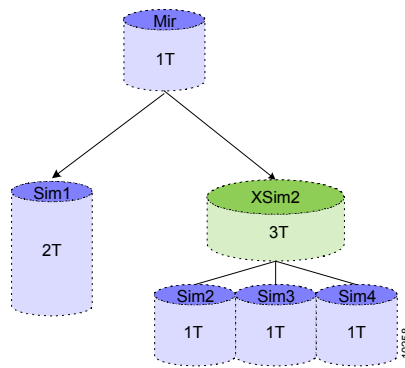


Figure 87. Further Resizing on the Same Volume

If a volume to be resized is a concatenated volume, a cube is not created and any volume type can be used except transparent or snapshot. In Figure 88, a concatenated volume with a potential capacity of two terabytes is resized to a potential capacity of three terabytes by the addition of a one-terabyte child without first creating a cube. The actual capacity of the concatenated volume remains unchanged until it is expanded to match its potential size.

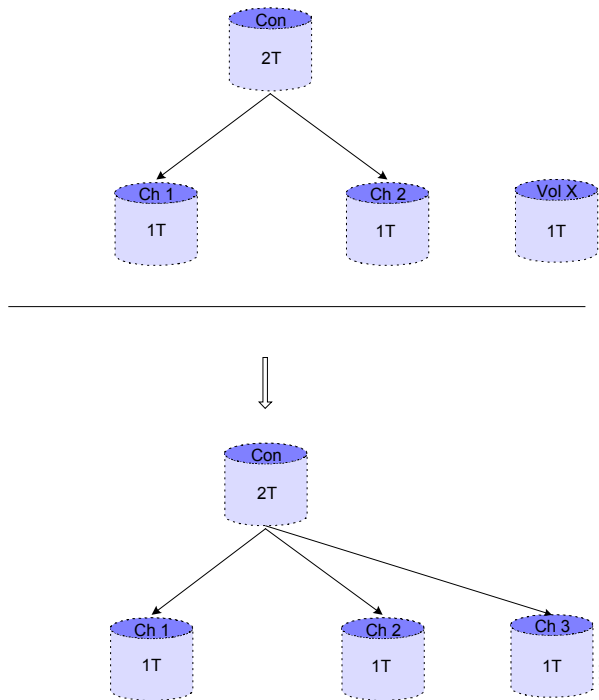


Figure 88. Resizing a Concatenated Volume

volume resize

You need to define three parameters to resize a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME TO RESIZE	MANDATORY	Ch2
-a	ALIAS	ALIAS OF RESIZED VOLUME	OPTIONAL IF NO NAME IS GIVEN, THE PREFIX X IS ADDED TO THE SOURCE NAME	XCh2
-with	VOLUME	VOLUME TO RESIZE WITH	MANDATORY	Sim

Example:

In Figure 89, page 157, the mirrored volume, Mir, is limited in its actual capacity by its smallest child, Sim2. To resize Sim2 to two terabytes, simple volume, Sim3, is concatenated to Sim2 to create the resized cube volume, XSim 2.

```
volume resize -vol Sim2 -a XSim2 -with Sim3
```

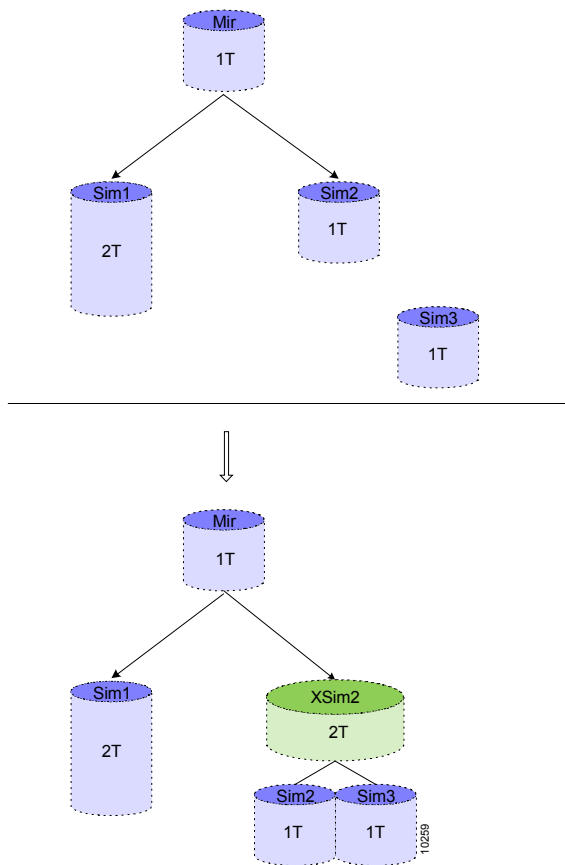


Figure 89. Resizing Mirrored Child

Retracting a Volume

After resizing a volume but before expanding its hierarchy, you can use the CLI command `volume retract` to delete the added volume(s) used to resize the original volume. The head of the volume hierarchy is retracted, not the resized volume.

`volume retract`

You need to define one parameter to retract a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME	VOLUME TO RETRACT – HEAD OF HIERARCHY	MANDATORY	Mir5

Expanding a Volume

If you are working in a V-Switch cluster, a volume must be expanded on both V-Switches.

You must expand a volume's actual capacity, its capacity as identified by the file server, to match its resized potential capacity using the CLI command `volume expand`. If you do not expand the resized volume, its resized capacity will not be available for storage use. After expanding a volume, its host's file server will show its new capacity but the disk partition will not expand automatically. The host must expand the disk partition.

In Figure 90, a concatenated volume is expanded from two terabytes to an actual capacity of three terabytes to match its resized potential capacity of three terabytes.

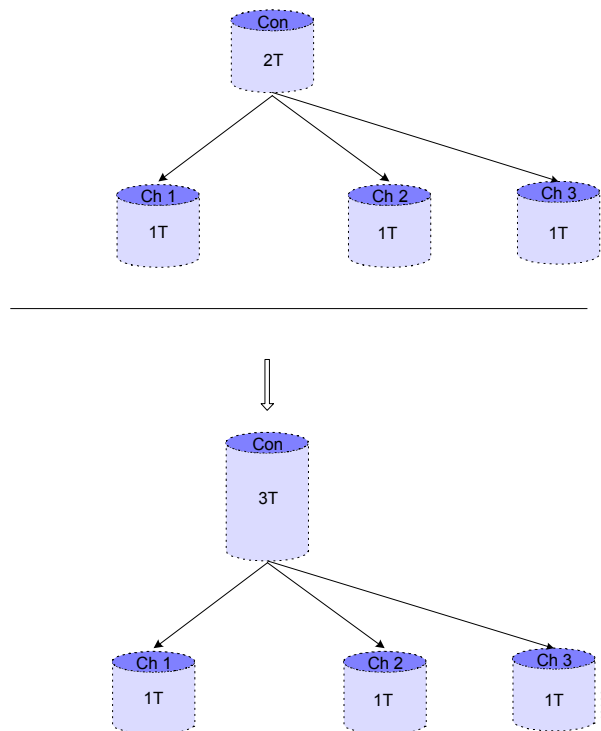


Figure 90. Expanding a Concatenated Volume

In Figure 91, page 159, a mirrored volume is expanded to two terabytes after one of its child volumes was resized and expanded to two terabytes.

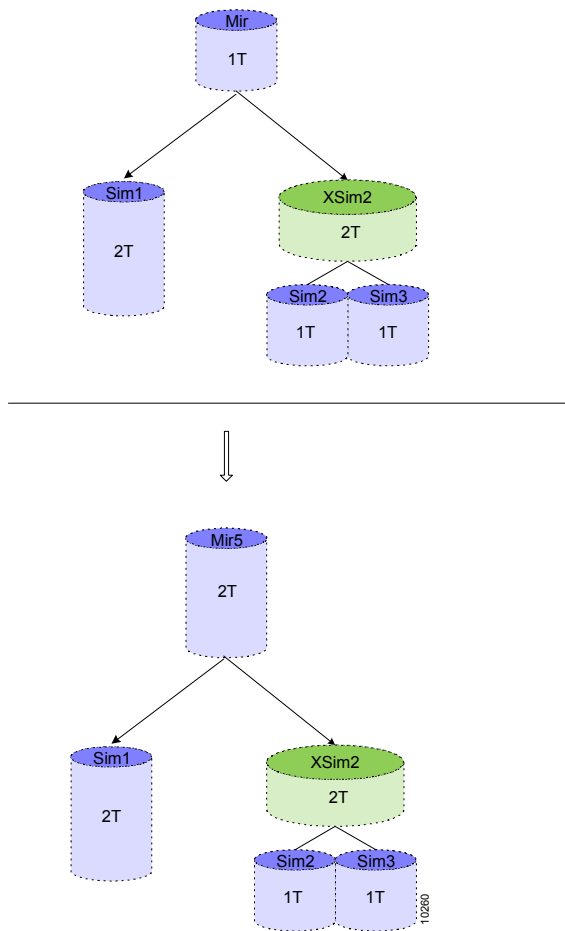


Figure 91. Expanding a Mirrored Volume

`volume expand`

You need to define one parameter to expand a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-vol</code>	VOLUME	VOLUME TO EXPAND	MANDATORY	XSim2

Example:

In Figure 92, page 160, the resized volume, XSim2, is expanded to an actual capacity of two terabytes to match its resized potential capacity. Once XSim2 is expanded, the capacity of Mir5 will automatically adjust itself to two terabytes.

`volume expand -vol XSim2`

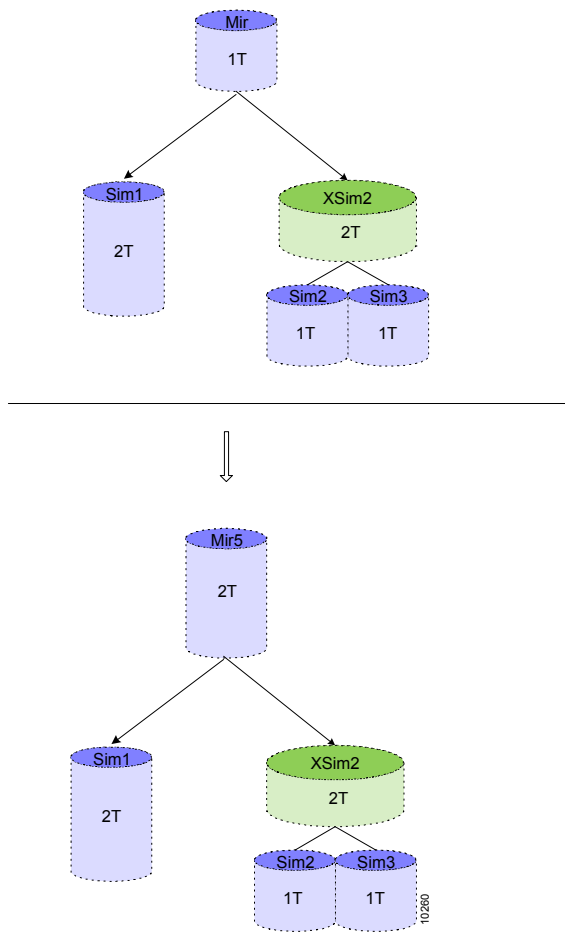


Figure 92. Expanding XSim2

User Notes



9

Routine Volume Maintenance

IN THIS CHAPTER

Once you have begun creating volumes and managing your storage, you may want to adjust or change certain parameters for more effective storage management and utilization.

VOLUMES

TARGETS AND EXPOSURE

This chapter explains how to rename or remove volumes, LUNs, iSCSI targets, identities and credentials.

Volumes

Renaming a Volume

If you are working in a V-Switch cluster, the volume must be renamed on both V-Switches.

After creating a volume you can rename it. Renaming a volume will have no negative effect on the volume hierarchies built on the renamed volume.

volume set

You need to define two parameters to rename a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME ALIAS	ALIAS OF VOLUME TO RENAME	MANDATORY	Concat1
-n	NEW ALIAS	NEW VOLUME ALIAS	MANDATORY	JPGRepos

Example:

```
volume set -vol Concat1 -n JPGRepos
```

Removing a Volume

If you are working in a V-Switch cluster, the volume must be removed on both V-Switches.

You can remove a volume. The volume must be inactive, that is not exposed, and it must be at the top level of its volume hierarchy. For example, you cannot remove a simple volume from within a set of volumes creating a striped volume. The striped volume is at the top of the hierarchy must be removed first.

volume remove

You need to define one parameter to remove a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME ALIAS	ALIAS OF TOP-LEVEL VOLUME TO REMOVE	MANDATORY	Stripe1

Example:

The top-level volume Stripe 1 is removed while the component volumes, Simple 2, 4, 8 & 10, remain intact.

```
volume remove -vol Stripe1
```

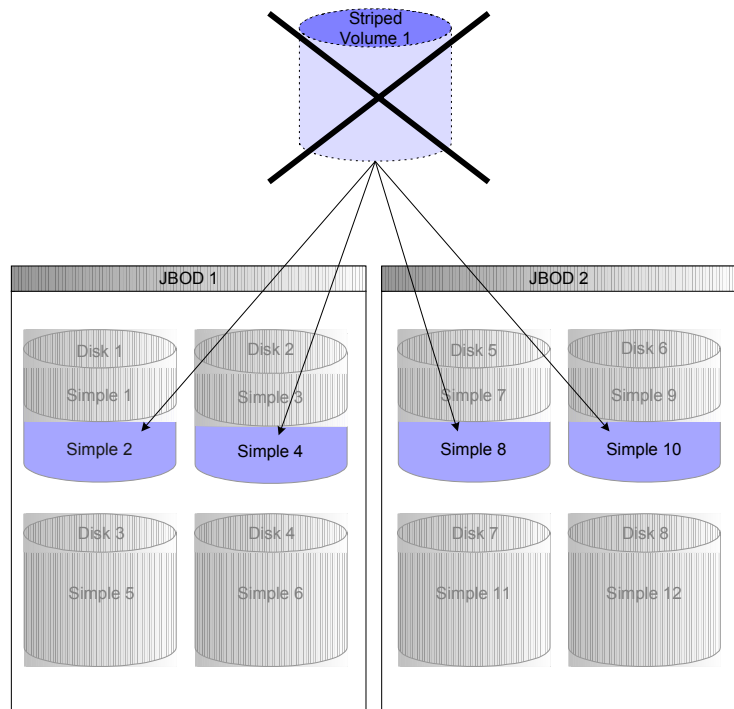


Figure 93. Stripe 1 Volume Removed

Removing all Volumes in a Hierarchy

If you are working in a V-Switch cluster, the volume must be removed on both V-Switches.

You can remove a volume and all of its component volumes in a volume hierarchy. The volume must be at the top of the hierarchy. The volume cannot be exposed; the volume LUN must be inactivated. Simple volumes will convert back to subdisks.

```
volume remove -all
```

You need to define one parameter to remove all volumes within a volume hierarchy:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-all	ALL	ALL VOLUMES IN HIERARCHY	MANDATORY	No parameter required
-vol	VOLUME ALIAS	ALIAS OF TOP-LEVEL VOLUME TO REMOVE	MANDATORY	Stripe1

Example:

The top-level volume Stripe 1 is removed along with its component volumes, Simple 2, 4, 8 & 10.

```
volume remove -all -vol Stripe1
```

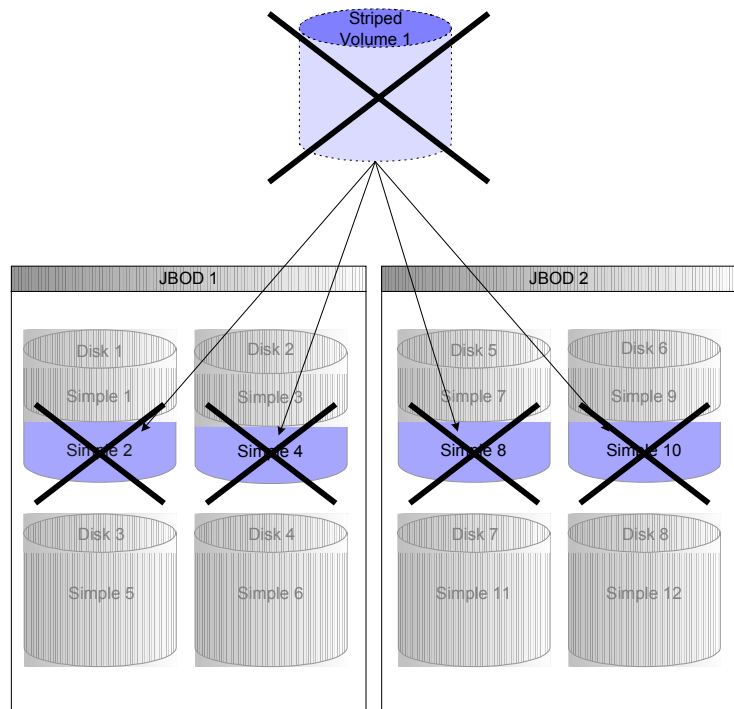


Figure 94. Stripe 1 Volume and Supporting Hierarchy Removed

Replacing a Volume

If you are working in a V-Switch cluster, the volume must be replaced on both V-Switches.

You can replace a volume with another volume. Use the CLI command **volume replace** after a disk failure to replace a volume used in a storage hierarchy with a volume on a functional disk. This is only a 'physical' replacement. The data on the failed disk is not copied to the new volume.

If you are replacing a volume used as part of a mirrored volume, continue with the CLI command **volume mirror synch** to synchronize the replacement volume with the other mirrored volume(s). See "Synchronizing a Volume," page 166.

volume replace

You need to define two parameters to replace a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME ON FAILED DISK	MANDATORY	Simple4
-nvol	NEW VOLUME	REPLACEMENT VOLUME	MANDATORY	Simple6

Synchronizing a Volume

You can replace a failed volume in a mirror. You must then synchronize the new volume to the original mirrored volumes. See the working example: “Replacing a Mirrored Volume,” page 256.

```
volume mirror sync
```

You need to define two parameters to synchronize a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE VOLUME	ORIGINAL VOLUME TO SYNCHRONIZE TO	MANDATORY	Simple3
-dst	DESTINATION VOLUME	NEW VOLUME TO ADD TO SYNCHRONIZE	MANDATORY	Simple5

Example:

The volume Simple3 is synchronized to the volume Simple5.

```
volume mirror sync -src Simple3 -dst Simple5
```

If you are working in a cluster, the volume will be displayed in the state need sync on both V-Switches. Synchronize the volume on the exposing V-Switch using the CLI command **volume mirror sync**. Perform a dummy synchronization on the non-exposing V-Switch using the CLI command **volume mirror dummysync**.

```
volume mirror dummysync
```

You need to define two parameters to dummy synchronize a volume:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	Mirror2
-dst	DESTINATION	ALIAS OF VOLUME TO COPY TO	MANDATORY	Mirror8

Targets and Exposure

Removing an LU

If you remove LU 0 from a target, you will inactivate the target even if the target has other attached LUs.

Before you can remove a volume, you must remove any attached LU.

```
lu remove
```

You need to define two parameters to remove an LU:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF TARGET FROM WHICH TO REMOVE LU	MANDATORY	Accounting
-lun	LOGICAL UNIT NUMBER	LU TO REMOVE FROM THE TARGET	MANDATORY	8

If you are working in a V-Switch cluster, the LU must be removed on both V-Switches.

Example:

```
lu remove -ta Accounting -lun 8
```

Changing iSCSI Target Parameters

If you are working in a V-Switch cluster, the target alias must be changed on both V-Switches.

This command renames a target alias. Renaming the alias will have no negative effect on the target exposure.

```
iscsi target set
```

You need to define two parameters to rename an iSCSI target alias:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF TARGET TO RENAME	MANDATORY	accounting
-na	NEW ALIAS	NEW ALIAS FOR TARGET	MANDATORY	finance

Example:

The target alias accounting is renamed to finance.

```
iscsi target set -ta accounting -na finance
```

Removing an iSCSI Target

If you are working in a V-Switch cluster, the target must be removed on both V-Switches.

You can remove an iSCSI target provided it has no attached LU. Use the CLI command `lu remove` to first remove any LUs from a target.

```
iscsi target remove
```

You need to define one parameter to remove an iSCSI target:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET TO REMOVE	MANDATORY	musicbox

Example:

```
iscsi target remove -ta musicbox
```

Removing a RADIUS Server

Use the CLI command `ip radius remove` to remove a RADIUS server from the V-Switch.

```
ip radius remove
```

You need to define one parameter to remove an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF RADIUS SERVER	MANDATORY	212.199.43.1
-p	PORT	UDP PORT FOR SENDING REQUESTS TO RADIUS SERVER	MANDATORY	1812

Removing an iSNS Server

Use the CLI command `ip isns remove` to remove an iSNS server from the V-Switch iSNS client.

```
ip isns remove
```

You need to define one parameter to remove an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1



10

Routine V-Switch Maintenance

IN THIS CHAPTER

Once you have configured the V-Switch, you need to be able to update its configuration and maintain optimum V-Switch functionality.

GENERAL CONFIGURATION PARAMETERS

This chapter explains how to modify configuration parameters; interface IP addresses, IP routing paths, cluster configurations and replace a power supply.

TELNET PORT

SNMP MANAGER

This chapter also explains how to upgrade the V-Switch software and reboot the V-Switch in safe mode.

ISNS SERVER

USER PROFILES

V-SWITCH

NETWORK INTERFACES

IP ROUTING

DISKS AND SUBDISKS

CLUSTERS

V-SWITCH 3000 POWER SUPPLY

UPGRADING THE V-SWITCH SOFTWARE

V-SWITCH 3000 COMPACT FLASH

SAFE MODE

General Configuration Parameters

This command is available only after the V-Switch is initialized with the `init` command.

After the initial V-Switch configuration, you may want to change one or more of the V-Switch parameters. For example: You may need to change the system clock to adjust to Daylight Savings Time. You can also use this command to add contact information of whom to contact in the event of technical difficulties.

`device set`

You can define or change thirteen parameters using this command:

If you are working in a V-Switch cluster, the changes must be configured in both V-Switches.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-n</code>	NAME	USER-ASSIGNED NAME FOR THE V-SWITCH	OPTIONAL	VSwitch1
<code>-ip</code>	MANAGEMENT IP ADDRESS	IP ADDRESS OF THE MANAGEMENT PORT	OPTIONAL	212.199.43.47
<code>-im</code>	MANAGEMENT IP MASK	IP MASK FOR THE MANAGEMENT PORT	OPTIONAL DEFAULT: 255.255.255.0	
<code>-p</code>	UDP PORT	PORT THROUGH WHICH ALL UDP COMMUNICATIONS WILL FLOW – NAMELY FOR SNMP	OPTIONAL DEFAULT: 161	
<code>-if</code>	INTERFACE ALIAS	ALIAS OF PORT FOR MANAGING V-SWITCH	OPTIONAL DEFAULT: MGMT (ETH1 OR MGMT)	
<code>-d</code>	DATE	LOCAL DATE	OPTIONAL	21/07/2002
<code>-t</code>	TIME	LOCAL TIME	OPTIONAL	13:30
<code>-c</code>	CONTACT	CONTACT PERSON IN THE EVENT OF A SYSTEM MALFUNCTION	OPTIONAL	AnnaLevin
<code>-loc</code>	LOCATION	LOCATION OF THE CONTACT PERSON	OPTIONAL	ext4838

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-rld	REPORT LUN DISCOVERY	MODE FOR DISCOVERING DEVICE LUNS	OPTIONAL YES OR NO DEFAULT: YES	no
-telnet	TELNET PORT	PORT FOR V-SWITCH COMMUNICATIONS	OPTIONAL DEFAULT: 23	1597
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	

Example:

The V-Switch is named V-Switch 1 at 13:30 in the afternoon on 21 March 2002. Its management port, eth1, has the IP address 212.199.43.46. Anna Levin, at phone extension 4838 is the contact person in the event of technical difficulties.

```
device set -n VSwitch1 -ip 212.199.43.46 -d 21/04/2004 -
t 13:30 -c AnnaLevin. -loc ext4838 -if eth1
```

Telnet Port

If you are working in a V-Switch cluster, the interface alias must be changed on both V-Switches.

If your Telnet communications connection to the V-Switch traverses a firewall, the standard Telnet communications port 23 may be blocked by the firewall as a security measure. To enable Telnet communications to the V-Switch, you can designate an alternate port using the CLI command **device set -telnet**. This port can be opened in the firewall for dedicated Telnet-V-Switch communications.

```
device set -telnet
```

Example:

The port 1597 is programmed as the Telnet communications port.

```
device set -telnet 1597
```

Use the CLI command **info** to check the V-Switch's designated Telnet port.

```
info
```

Table 29: V-Switch Configuration

Parameter	Value
Name	VSwitch1
Description	SDC HW 1.0 SW 1.0
Contact	Anna Levin
Location	Ext. 4838
Status	OK
Object ID	1.3.6.1.4.1 10059 1.1.2
Time Since Last Reset	12 days 17 hours 29 min 32 sec
Mgmt IP Address	212.199.43.47
Mgmt UDP Port	161
Date & Time [DD/MM/YY]	21/04/04 13:33
Telnet Port	1597
Eth	Up
FC	Up
Read Community	Public
Write Community	Private

SNMP Manager

Setting an SNMP Manager

This command modifies parameters of existing managers.

snmp manager set

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UPD PORT	PORT TO RECEIVE TRAPS THROUGH	OPTIONAL DEFAULT: 162	150
-np	NEW PORT	NEW PORT FOR RECEIVING TRAPS	OPTIONAL	151
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	
-trap	TRAP	TO SEND TRAPS TO MANAGER	OPTIONAL YES: SEND NO: DO NOT SEND DEFAULT: YES	

Removing an SNMP Manager

This command removes a manager from the V-Switch.

snmp manager remove

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UDP PORT	PORT TO RECEIVE TRAPS THROUGH	MANDATORY	162

iSNS Server

The V-Switch supports Internet Storage Name Service (iSNS) protocol for advertising its targets and portals on the iSNS server to enable iSCSI initiators in the IP-SAN to locate the V-Switch targets automatically.

Adding an iSNS Server

Use the CLI command `ip isns add` to add an iSCSI server to the V-Switch's iSNS client. Targets defined by the V-Switch's Access Control List (ACL) as having controlled access are accessible only to those servers defined as having access to the target

```
ip isns add
```

You need to define one parameter to add an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1

Removing an iSNS Server

Use the CLI command `ip isns remove` to remove an iSNS server from the V-Switch iSNS client.

```
ip isns remove
```

You need to define one parameter to remove an iSNS server address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1

User Profiles

Access to the V-Switch is password protected. The V-Switch ships with the default user name sanrad and the default user password sanrad. After logging in, a total of ten user profiles (name plus password) can be configured on a V-Switch. As needed, profiles can be modified or removed.

The user name can have from one to twenty characters. The user password can have from six to twelve characters. Both fields are case sensitive and accept all characters, including spaces.

Adding a User Profile

All CLI names and aliases are case sensitive.

A total of ten user profiles can be configured on a V-Switch. Use the CLI command `admin add` to add a user login profile

```
admin add
```

You must define two parameters to add a user profile:

If you are working in a V-Switch cluster, a user profile must be added on both V-Switches.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-un	USER NAME	USER NAME	MANDATORY	Joe Cool
-pw	PASSWORD	USER PASSWORD	MANDATORY	123456

Example:

```
admin add -un Joe Cool -pw 123456
```

Changing a User Profile

If you are working in a V-Switch cluster, a user profile must be changed on both V-Switches

This interactive command enables a user to change their login password for their user name on the V-Switch.

```
admin password
```

After entering the command, you are prompted to enter your existing password and the new password.

Removing a User Profile

If you are working in a V-Switch cluster, a user profile must be changed on both V-Switches

You can remove any user profile from the V-Switch database except the profile you are logged in with. This ensures at least one user profile in the database at all times.

```
admin remove
```

You must define one parameter to remove a user profile:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-un	USER NAME	USER NAME	MANDATORY	Joe Cool

Example:

```
admin remove -un Joe Cool
```

V-Switch

Resetting a V-Switch

You can perform a remote soft reset on the V-Switch using the CLI **reset** command. All configuration databases will be maintained on the V-Switch, including user names and passwords; network port aliases; configured volumes and iSCSI targets.

```
reset
```

Saving (Uploading) a V-Switch Database File

You can upload a copy of a V-Switch's full database file to the local TFTP server. If the V-Switch fails, its database file can be downloaded to the replacement V-Switch. This eliminates protracted configuration time on the new V-Switch and ensures configuration integrity.

Use the CLI command **ft upload** to upload a V-Switch's full database file

```
ft upload
```

You need to define three parameters to upload a database file:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF STATION WHERE TFTP APPLICATION SITS	MANDATORY	212.199.43.70
-fn	FILE NAME	COMPLETE PATH AND NAME TO SAVE FILE AS	MANDATORY	VSwitch/v1_9/v1_9database
-ft	FILE TYPE	FORMAT TO SAVE DATA IN	OPTIONAL DEFAULT: DB (DATA BASE)	db

Example:

Upload the file v1_9dat as a database file to the tftp server at 212.199.43.70.

```
ft upload -ip 212.199.43.70 -fn VSwitch/v1_9/v1_9database -ft db
```

Downloading a V-Switch Configuration File

Download the database file to the V-Switch before attaching it to the storage devices.

After replacing a failed V-Switch, you can download the replaced V-Switch database file from the tftp server to the new V-Switch. Unlike a standard V-Switch installation, do not connect the V-Switch to the storage devices before powering up. You first download the database file and then connect the V-Switch to the storage devices. This ensures that autodiscovery will not assign default aliases different from the replaced V-Switch to the discovered disks.

The V-Switch must be reset for the downloaded database to become operational.

Use the CLI command **ft download** to download a V-Switch database file from the local TFTP server after you have initialized the replacement V-Switch with an IP management address via LCD or Console.

Please refer to “Configuring the V-Switch 3000 Management Parameters via LCD,” page 48, and “Configuring the Management Console,” page 49, for more information on initializing your V-Switch before downloading the configuration file.

The download parameters are identical to the upload parameters.

ft download

You need to define three parameters to download a configuration file:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	212.199.43.70
-fn	FILE NAME	COMPLETE PATH AND NAME TO FILE LOCATION	MANDATORY	VSwitch/v1_9/v1_9database
-ft	FILE TYPE	FORMAT TO SAVE DATA IN	OPTIONAL DEFAULT: DB (DATA BASE)	db

Example:

Download the file v1_9database as a database file from the tftp server at 212.199.43.70.

```
ft download -ip 212.199.43.70 -fn VSwitch/v1_9/v1_9database -ft db
```

Network Interfaces

Changing an Interface Alias

All CLI names and aliases are case sensitive.

You can change the alias of a V-Switch interface for user convenience. Leaving the new alias field blank will return the alias to its default setting

```
interface set
```

You need to define two parameters to change an interface alias:

If you are working in a V-Switch cluster, the interface alias must be changed on both V-Switches.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE ALIAS OR NAME	CURRENT ALIAS OR NAME OF INTERFACE	MANDATORY	fc1
-na	NEW ALIAS	NEW ALIAS OR NAME OF INTERFACE	OPTIONAL DEFAULT: DEFAULT INTERFACE NAMES – CONS, MGMT, FC1,SCSI1,ETH1	Storage1

Example:

The storage interface, fc1 is renamed to Storage 1.

```
interface set -if fc1 -na Storage1
```

Adding an Interface IP Address

If you are working in a V-Switch cluster, the interface IP must be added on both V-Switches.

You can assign more than one IP address to each network port.

```
ip config set
```

You need to define three parameters to configure each network port:

Executing this command on the same network port with a different IP address will not reset the network port address. It will add another IP address to the network port

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE ALIAS	NETWORK INTERFACE PORT	MANDATORY ETH1, ETH2, ETH3	eth1
-ip	IP ADDRESS	IP ADDRESS ASSIGNING TO THE INTERFACE PORT	MANDATORY	212.199.43.57
-im	IP MASK	IP NET MASK	OPTIONAL DEFAULT: 255.255.255.0	
-act	ACTIVITY	IF IP ADDRESS IS ACTIVE TO EXPOSE VOLUMES. USE INACTIVE STATUS TO ALLOW FAILOVER.	OPTIONAL DEFAULT: 1 (ACTIVE). 2(INACTIVE)	1

Example:

IP address 212.199.43.57 is added to interface eth1 for a total of two IP addresses assigned to interface eth1.

```
ip config set -if eth1 -ip 212.199.43.57
```

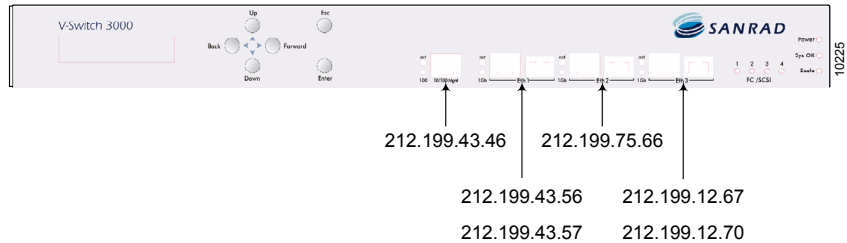


Figure 95. Adding an Interface IP Address

Removing an Interface IP Address

If you are working in a V-Switch cluster, the interface IP must be removed on both V-Switches.

You can remove an IP address from the network ports.

```
ip config remove
```

You need to define one parameter to remove a network port IP address:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS TO REMOVE FROM THE NETWORK INTERFACE PORT	MANDATORY	212.199.12.70

Example:

The second IP address, 212.199.43.70, on the network interface eth3 is removed.

```
ip config remove-ip 212.199.12.70
```

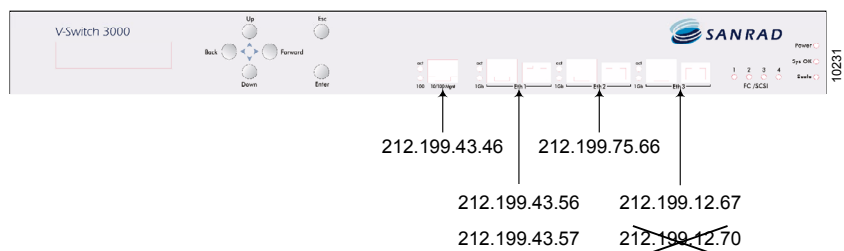


Figure 96. Removing an IP Address

IP Routing

Adding an IP route

If you are working in a V-Switch cluster, the IP route must be added on both V-Switches.

You can add an IP route to a network port.

```
ip route add
```

You need to define four parameters to add an IP route:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-dip	DESTINATION IP	IP OF HOST STATION	MANDATORY	10.10.20.20
-dmask	DESTINATION MASK	IP MASK OF HOST STATION	MANDATORY	255.255.255.0
-gw	GATEWAY IP ADDRESS	IP ADDRESS OF THE GATEWAY ROUTER	MANDATORY	30.30.20.20
-if	INTERFACE ALIAS	NETWORK PORT TO OPEN COMMUNICATION THROUGH	MANDATORY	eth2

Example:

An IP routing path to Network D, IP 10.10.20.20, (IP mask 255.255.255.0) is mapped from network port Eth2 through router gateway 30.30.20.20.

```
ip route add -dip 10.10.20.20 -dmask 255.255.255.0 -gw 30.30.20.20 -if eth2
```

Removing an IP route

If you are working in a V-Switch cluster, the IP route must be removed on both V-Switches.

You can remove an IP route to a network.

```
ip route remove
```

You need to define four parameters to remove an IP routing path

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-dip	DESTINATION IP	DESTINATION NETWORK IP ADDRESS	MANDATORY	10.10.20.20
-dmask	DESTINATION MASK	DESTINATION NETWORK IP MASK	MANDATORY	255.255.255.0

-gw	GATEWAY IP ADDRESS	IP ADDRESS OF THE GATEWAY ROUTER	MANDATORY	30.30.20.20
-if	INTERFACE ALIAS	INTERFACE ALIAS ROUTING PATH MAPS TO	MANDATORY	eth2

Example:

The IP route from network port Eth2 to external network 10.10.20.20, with IP mask 255.255.255.0 is removed from Eth2.

```
ip route remove -dip 10.10.20.20 -dmask 255.255.255.0
-gw 30.30.20.20 -if eth2
```

Disks and Subdisks

Discovering Storage Devices

The V-Switch default algorithm for storage devices discovery is using the SCSI command REPORT LUNS. Certain storage devices either do not support this command or do not respond according to the SCSI standard. To discover these devices, the REPORT LUNs command must be disabled. If certain devices in the SAN are not being discovered by the V-Switch, use the CLI command **device set** to disable or re-enable device discovery via REPORT LUNs.

device set

You need to define one parameter to change the V-Switch storage device discovery mode:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-rld	REPORT LUN DISCOVERY	MODE FOR DISCOVERING DEVICE LUNS	MANDATORY YES OR NO DEFAULT: YES	no

See “device set,” page 200, for the full list of switch parameters for the CLI command **device set**.

Renaming a Storage Device

If you are working in a V-Switch cluster, the disk must be renamed on both V-Switches.

You can rename a disk. Renaming the disk will have no effect on the volume hierarchies built on the disk.

storage set

You need to define three parameters to rename a disk:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE ALIAS	STORAGE ALIAS TO MODIFY	MANDATORY	Stor_1
-na	NEW ALIAS	NEW ALIAS FOR STORAGEK	MANDATORY IF CHANGING	RAID1
-info	INFORMATION	INFORMATION TO ASSIGN TO STORAGE DEVICE	MANDATORY IF CHANGING	Expose_as _transparent

Example:

The disk, **Stor_1**, is renamed to **RAID1** and a note is made for the storage manager to expose this disk as a transparent volume.

```
storage set -s Stor_1 -na RAID1 -info Expose_as  
_transparent
```

Removing a Storage Device

If you are working in a V-Switch cluster, the disk must be removed on both V-Switches.

You can remove a disk from the V-Switch database. The disk must be defined as missing to remove it.

```
storage remove
```

You need to define one parameter to remove a disk:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE	ALIAS OF STORAGE TO REMOVE	MANDATORY	Stor_1

Example:

Disk named Stor_1 is removed from the V-Switch database.

```
storage remove -s Stor_1
```

Renaming a Subdisk

If you are working in a V-Switch cluster, the subdisk must be renamed on both V-Switches.

After creating a subdisk you can rename it. Renaming the subdisk will have no effect on the volume hierarchy built on the subdisk.

```
subdisk set
```

You need to define three parameters to rename a subdisk:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-sd	SUBDISK ALIAS	ALIAS OF SUBDISK TO RENAME	MANDATORY	Subdisk7
-na	NEW SUBDISK ALIAS	NEW ALIAS OF SUBDISK	MANDATORY	Sub7
-info	INFORMATION	INFORMATION ON SUBDISK FOR LOCAL ADMINISTRATION ONLY	OPTIONAL	replaces_sub3

Removing a Subdisk

If you are working in a V-Switch cluster, the subdisk must be removed on both V-Switches

You can remove a subdisk to repartition a disk.

```
subdisk remove
```

You need to define one parameter to remove a subdisk:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-sd	SUBDISK ALIAS	ALIAS OF SUBDISK TO DELETE	MANDATORY	Subdisk4

Clusters

Modifying Neighbor Parameters

You can modify neighbor parameters in a cluster.

`neighbor set`

You need to define up to two parameters to modify a neighbor's parameters in a cluster:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBORING V-SWITCH IN CLUSTER	MANDATORY IF CHANGING	NewVSwitch
-ip	IP ADDRESS	MANAGEMENT IP ADDRESS OF NEIGHBOR	MANDATORY IF CHANGING	212.199.43.40

Removing a Neighbor

Both V-Switches must have its neighbor removed.

You can remove a neighbor from a cluster.

`neighbor remove`

You need to define one parameter to remove a neighbor from a cluster:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBORING V-SWITCH IN CLUSTER	MANDATORY IF CHANGING	NewVSwitch

Modifying a Cluster

Both V-Switches in the cluster must be modified.

You can modify a cluster's parameters.

cluster set

You need to define three parameters to modify a cluster's parameters:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-kai	KEEP ALIVE INTERVAL	TIME BETWEEN ALIVE SIGNALS FROM NEIGHBORS	MANDATORY IF CHANGING	5
-sint	SUSPICIOUS INTERVAL	TIME FROM WHEN A SIGNAL WAS EXPECTED BUT NOT RECEIVED	MANDATORY IF CHANGING	10
-fint	FAILOVER INTERVAL	TIME WHEN SUSPICIOUS INTERVAL IS EXCEEDED	MANDATORY IF CHANGING	10

Enabling and Disabling Failover

If you want to break a cluster or need to take a V-Switch off-line, you must first disable V-Switch failover. Use the CLI command **cluster failover disable** to disable this functionality. This command must be executed on both V-Switches in the cluster.

```
cluster failover disable
```

If you want to restore a cluster or after you bring the V-Switch back on-line, you need to re-enable the failover functionality. Use the CLI command **cluster failover enable** to re-enable this functionality. This command must be executed on both V-Switches in the cluster.

```
cluster failover enable
```

V-Switch 3000 Power Supply

The V-Switch 3000 is standard-issued with two hot-swappable AC power supplies. If one of the power supplies fail, its red LED on the back panel turns off. If both of the power supplies fail, the Power LED on the front panel turns off.

STEP 1. DISCONNECT THE POWER CABLE

Disconnect the power cable from the power source. After the power cable is disconnected from the power source, disconnect the power cable from the V-Switch.

STEP 2. LOOSEN THE POWER SUPPLY CONNECTING SCREW

Loosen the power supply connecting screw to release the power supply from the V-Switch.

STEP 3. REMOVE THE POWER SUPPLY

Lift the power supply handle and pull to slide the power supply out

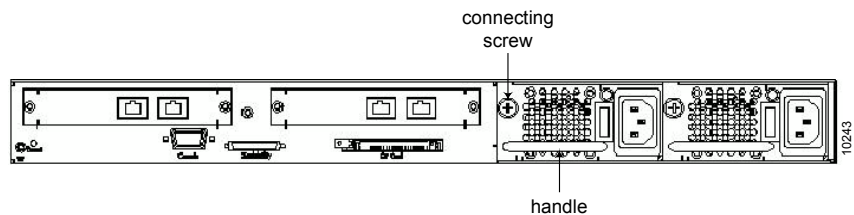


Figure 97. Replacing a Power Supply

STEP 4. INSERT A FUNCTIONING COMPATIBLE POWER SUPPLY AND SECURE

Insert a functioning compatible power supply. Secure the power supply to the V-Switch.

It is now safe to reconnect the power cable to the power supply and power source.

Upgrading the V-Switch Software

The V-Switch must be reset for the new software to begin functioning.

You can upgrade the V-Switch software via CLI. The software upgrade files are first downloaded from the TFTP server. You can then use the CLI command `ft update` to upgrade the V-Switch software. There are a total of six upgrade files. Do not change their names or the V-Switch will not be able to perform the upgrade.

All configured user profiles are unaffected by the software upgrade.

`ft update`

You need two parameters to upgrade the V-Switch software:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	TFTP SERVER IP ADDRESS	MANDATORY	212.199.43.46
-fd	DIRECTORY	DIRECTORY TO TAKE FILES FROM	OPTIONAL	sanrad/update/v2_0/

Example:

```
ft update -ip 212.199.43.46 -fd sanrad/update/v2_0/
```

After upgrading the software, the V-Switch must be reset for the new software to begin functioning. Use the CLI command `reset` to reset the V-Switch.

`reset`

Use the CLI command `info` to view the software version to confirm that the software has successfully upgraded.

V-Switch 3000 Compact Flash

The V-Switch 3000 includes a compact flash for backing up the database to provide redundancy and for backing up the application before upgrading the software. The V-Switch 3000 has two permanent memory devices: flash and compact flash. The V-Switch can work with only the flash. When both are present, the V-Switch reads from the flash and can be set to write to both the flash and the compact flash. Use the CLI command **system set** to replicate the database from the flash on to the compact flash.

When set to replicate mode, the V-Switch copies the current database from the flash to the compact flash. Any configuration changes done to the database will automatically be updated to the compact flash as well.

system set

You need to define one parameter to set the replication mode:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-rep	REPLICATE	REPLICATION OF THE DATABASE	MANDATORY YES: REPLICATE NO: DO NOT REPLICATE	yes

system set -rep yes

If the compact flash is removed while the V-Switch is in replicate mode, it will automatically switch to non-replicate mode, even if the compact flash is re-inserted. Repeat the command **system set** to return to replicate mode.

At initialization in replication mode, the V-Switch checks both copies of the database. If they are different, the V-Switch switches to non-replicate mode to prevent erasing the compact flash.

The V-Switch's database, application and configuration files can also be copied from flash to compact flash or compact flash to flash. Use the CLI command **system copy** to copy each file type separately.

Use the CLI command **system copy** to copy a file between the flash and the compact flash.

system copy

You need to define two parameters to copy a file between the flash and compact flash:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-from	FROM	WHERE TO COPY FROM	MANDATORY FLASH CFLASH	cflash
-type	TYPE	TYPE OF FILE TO COPY	MANDATORY DB: DATABASE AF: APPLICATION FILE CF: CONFIGURATION FILE	db

```
system copy -from cflash -type db
```

Safe Mode

The V-Switch operating status includes the ability to enter into safe mode in the event of booting problems or in an attempt to clear significant amounts of a V-Switch configuration. There are two ways to enter safe mode:

- Automatically during a reboot.
- Manually via CLI.

There are four safe mode reboot options:

- Level 0: Reboot in normal mode.
- Level 1: Reboot with last good configuration.
- Level 2: Reboot with default factory database.
- Level 3: Reboot with default factory system.

Automatic Safe Mode

When the V-Switch reboots, either after upgrading the V-Switch software or any other time that environmental irregularities require, there may be database corruption. To prevent potential damage to the database, the V-Switch enters safe mode.

Safe mode can only be navigated from a console with a local, direct RS232 connection to the V-Switch.

When a V-Switch has boot problems and enters safe mode, its LCD panel displays:

```
Init Problem
Safe Mode
```

Level 0: Reboot in Normal Mode

If the V-Switch is rebooted during initialization it will reboot in safe mode 0. This gives the V-Switch another opportunity to try to reboot normally in the event that there are in fact no problems with the database.

Level 1: Reboot with Last Good Configuration

Save the V-Switch configurations to the database as the last good configuration by reboot after major configurations.

Each time the V-Switch successfully boots up, it saves the database as the last good configuration. If the last time the V-Switch booted was also the first time the V-Switch booted, the database will be empty. All V-Switch configurations will be lost. Therefore, SANRAD strongly urges you to reboot the V-Switch after major configurations to save the configuration database in the event of rebooting problems in the future.

Rebooting with the last good configuration may cause data corruption. For example, the last good configuration may contain a striped volume composed of two children. Since the last good configuration, that striped volume has been reconfigured to include three children. If the V-Switch

reboots with the last good configuration, all data written on the third child will be lost.

The suspicious database is saved and can then be exported to SANRAD technical support for examination using the CLI command `ft export problem` after initializing the V-Switch. Please see “Level 4:

Level 5:

If the V-Switch enters a reboot loop, after a given number of times, the reboot loop will be stopped and the V-Switch will enter safe mode 5. A reboot loop is most often caused by the connection of a problematic device to the V-Switch. In addition to contacting Technical Support, SANRAD recommends disconnecting storage and Ethernet connections and rebooting the V-Switch. If the V-Switch reboots without problems, an attached device is the culprit.

Exporting a Corrupted Database,” page 191.

Level 2: Reboot with Default Factory Database

This does not clear user login profiles.

This is the recommended option.

This clears the database of all configurations that may have been done, e.g. IP addresses, subdisks, volumes and targets. The suspicious database is copied to the directory **corrupted database** where it can then be exported to SANRAD technical support for examination using the CLI command **ft export problem** after initializing the V-Switch.

Level 3: Reboot with Default Factory System

This clears all user login profiles. You will have to login with the user name sanrad and password sanrad.

This clears the database of all configurations executed on the V-Switch, including user login profiles. You will have to log in with the user name sanrad and password sanrad.

Level 4:

Level 5:

If the V-Switch enters a reboot loop, after a given number of times, the reboot loop will be stopped and the V-Switch will enter safe mode 5. A reboot loop is most often caused by the connection of a problematic device to the V-Switch. In addition to contacting Technical Support, SANRAD recommends disconnecting storage and Ethernet connections and rebooting the V-Switch. If the V-Switch reboots without problems, an attached device is the culprit.

Exporting a Corrupted Database

After you reboot the V-Switch from safe mode level 1 or 2, you can use the CLI command `ft export problem` to export the potentially corrupted database to SANRAD technical support for examination.

If you rebooted in safe mode level 1 (last good configuration), the last good database file and the corrupted database file are exported for examination.

If you rebooted in safe mode level 2 (reboot with default factory database), the corrupted database file is exported for examination.

`ft export problem`

You need two parameters to export a corrupted database from the V-Switch:

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-ip</code>	IP ADDRESS	SERVER IP ADDRESS	MANDATORY	<code>212.199.43.70</code>
<code>-fd</code>	FILE DIRECTORY	DIRECTORY TO EXPORT FILES TO	MANDATORY	<code>Corrupted_DB</code>

Example

The suspicious database is exported to the directory `Corrupted_DB` at IP address `212.199.43.70`.

```
ft export problem -ip 212.199.43.70 -fd Corrupted_DB
```

Manual Safe Mode

You can use the CLI to clear a V-Switch's database to varying degrees. This is useful if you want to change the physical storage pool managed by a V-Switch or make substantial changes to the virtualization configuration.

Safe mode levels 0 and 1 can be executed from any Telnet station but, for extra safety, safe mode levels 2 and 3 can only be executed from a console with a local, direct RS232 connection to the V-Switch.

`system boot`

You need one parameter to reboot the V-Switch in safe mode.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
--------	-----------	------------	--------	---------

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
- sm	SAFE MODE	SAFE MODE LEVEL	MANDATORY	1
			0: NORMAL 1: LAST GOOD CONFIGURATION 2: DEFAULT DATABASE 3: DEFAULT FACTORY SYSTEM	

Level 0: Normal Mode

This is the same as resetting the V-Switch. No change is made to the V-Switch configuration.

Level 1: Last Good Configuration

Each time the V-Switch successfully boots up, it saves the database as the last good configuration. If the last time the V-Switch booted was also the first time, the database will be empty. Use this level to erase all configurations executed since the last reboot and return to the previous V-Switch configuration.

For example, if you are modifying or making temporary changes to the V-Switch configuration, first ensure that the current configuration is stored in the V-Switch by resetting the V-Switch then execute the changes. If the changes are no longer desirable, reboot in this level.

Level 2: Default Factory Database

A direct RS232 connection is necessary.

This clears the database of all configurations except user login profiles. Use this level to erase all virtual configurations except the user profiles.

For example, if you want to transfer the V-Switch to a different physical storage pool within a campus, this level will prepare the V-Switch for its new configuration while maintaining the same user profiles of the same system administrators.

Level 3: Default Factory System

A direct RS232 connection is necessary.

This clears the database of all configurations executed on the V-Switch, including user login profiles. Use this level if you want to completely clear a V-Switch's database.

For example, if you want to transfer a V-Switch to another branch office or campus department with different system administrators, this level will return the V-Switch to the same state it left the factory for shipping.

User Notes



11

Command Line Interface

IN THIS CHAPTER

V SWITCH
CONFIGURATION

VOLUME
CONFIGURATION

VOLUME EXPOSURE

The CLI is available via:

- ❑ Console port with a direct RS232 connection.
- ❑ 1Gbit Ethernet network port (eth1) with a Telnet session.
- ❑ 10/100 Ethernet Management port with a Telnet session.

The CLI is used to implement all V Switch management functions, including switching, virtualization and security.

All CLI commands are case sensitive and must be entered in lower case. Inputted data can include upper case letters but must always subsequently be entered in the same case.

The CLI command prompt is >.

All CLI commands in this manual are listed first with the basic command followed by a table of command switches; their explanations; status (mandatory or optional) and an example for each command switch.

The CLI supports the use of the following hot keys for the listed functions:

Table 30: Hot Keys

Command	Description
?	LIST OF COMMANDS WITH A SHORT DESCRIPTION OF EACH
!	RETURN TO MAIN MENU
Esc	ABORT CURRENT COMMAND
#	DISPLAY LAST COMMAND TO VIEW COMMAND HISTORY
Tab	COMPLETE A COMMAND TO THE POINT OF AMBIGUITY

V Switch Configuration

These commands enable you to configure and view the basic V Switch parameters needed to operate the V Switch

COMMAND	COMMAND
INIT	IP CONFIG REMOVE
ADMIN SHOW	IP ROUTE ADD
ADMIN ADD	IP ROUTE SHOW
ADMIN REMOVE	IP ROUTE REMOVE
ADMIN PASSWORD	IP ISNS SHOW
RESET	IP ISNS ADD
INFO	IP ISNS REMOVE
DEVICE SET	NEIGHBOR ADD
DEVICE SET -TELNET	NEIGHBOR SET
FC INTERFACE SHOW	NEIGHBOR SHOW
FC NODE SHOW	NEIGHBOR DETAILS
FC SET SPEED	NEIGHBOR REMOVE
INTERFACE SHOW	CLUSTER SHOW
INTERFACE DETAILS	CLUSTER SET
INTERFACE SET	CLUSTER FAILOVER ENABLE
PSCSI SHOW	FT SHOW
PSCSI SET BUSID	FT DOWNLOAD
SNMP MANAGER SHOW	FT EXPORT PROBLEM
SNMP MANAGER ADD	SYSTEM BOOT
SNMP MANAGER SET	SYSTEM SET
SNMP MANAGER REMOVE	SYSTEM COPY
IP CONFIG SHOW	SYSTEM SHOW
IP CONFIG SET	

init

This command initializes the most basic V Switch parameters needed to begin managing the V Switch operations via the management port. This command is executed via RS232 connection to a console.

This command can only be executed once. This command is unavailable once the basic V Switch parameters are set.

If the V Switch management IP address and mask are set using the LED, the V Switch name is set to the default **V Switch** and this command will not be available. Use the CLI command **device set** to change the basic V Switch parameters.

init

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-n	NAME	USER-ASSIGNED NAME FOR THE V SWITCH	MANDATORY	VSwitch1
-ip	MANAGEMENT IP ADDRESS	IP ADDRESS OF THE MANAGEMENT PORT	MANDATORY	212.199.43.46
-im	MANAGEMENT IP MASK	IP MASK FOR THE MANAGEMENT PORT	OPTIONAL DEFAULT: 255.255.255.0	
-p	UDP PORT	PORT THROUGH WHICH ALL UDP COMMUNICATIONS WILL FLOW – NAMELY FOR SNMP	OPTIONAL DEFAULT: 161	
-if	INTERFACE ALIAS	ALIAS OF MANAGEMENT INTERFACE	OPTIONAL DEFAULT : ETH1	

Example

```
init -n VSwitch1 -ip 212.199.43.46
```

admin show

This command shows all valid user login names for the V Switch.

admin show

Table 31: Administrator User Names

User Name
Joe Cool
Cyber Dude

User Name
MI5
CUL8R
C6H12O6

admin add

This command adds a user name to the list of valid user login names for the V Switch. A user name can be from 1 to 20 characters long, including spaces. A password can be from 6 to 12 characters long, including spaces.

`admin add`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-un	USER NAME	USER NAME	MANDATORY	Joe Cool
-pw	PASSWORD	USER PASSWORD	MANDATORY	123456

Example

```
admin add -un Joe Cool -pw 123456
```

admin remove

This command deletes a user name from the list of valid user login names for the V Switch. Any user name, except the logged in user name, can be deleted.

`admin remove`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-un	USER NAME	USER NAME	MANDATORY	Joe Cool

Example

```
admin remove -un Joe Cool
```

admin password

This interactive command enables a user to change their login password for their user name on the V Switch. You can only change the password of the current active user.

`admin password`

reset

This command performs a remote soft reset of the V Switch. All configuration databases will be maintained on the V Switch, including user names and passwords; network port aliases; configured volumes and iSCSI targets.

```
reset
```

info

This command displays the current V Switch configuration, including whom to contact in the event of technical difficulties.

```
info
```

Table 32: iSCSI V Switch Configuration

Parameter	Value
Name	V Switch1
Description	High Performance V Switch
Contact	Anna Levin
Location	Ext. 4838
Status	OK
Object ID	1.3.6.1.4.1.10059.1.1.2
Time Since Last Reset	5 days 1 h:29 m:49 sec
Mgmt IP Address	212.199.43.46
Mgmt UDP Port	161
Date & Time	24/03/02 15:37
Telnet Port	23

device set

This command redefines the specified general parameters of the V Switch.

```
device set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-n	NAME	USER-ASSIGNED NAME FOR THE V SWITCH	OPTIONAL	VSwitch1
-ip	MANAGEMENT IP ADDRESS	IP ADDRESS OF THE MANAGEMENT PORT	OPTIONAL	212.199.43.46
-im	MANAGEMENT IP MASK	IP MASK FOR THE MANAGEMENT PORT	OPTIONAL DEFAULT: 255.255.255.0	

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-p	UDP PORT	PORT THROUGH WHICH ALL UDP COMMUNICATIONS WILL FLOW – NAMELY FOR SNMP	OPTIONAL DEFAULT: 161	
-d	DATE	LOCAL DATE	OPTIONAL	21/04/2002
-t	TIME	LOCAL TIME	OPTIONAL	13:30
-c	CONTACT	CONTACT PERSON IN THE EVENT OF A SYSTEM MALFUNCTION	OPTIONAL	AnnaLevin
-loc	LOCATION	LOCATION OF THE CONTACT PERSON	OPTIONAL	ext4838
-if	MANAGEMENT INTERFACE ALIAS	MANAGEMENT PORT NAME	MANDATORY ETH1	eth1
-rld	REPORT LUN DISCOVERY	MODE FOR DISCOVERING DEVICE LUNS	MANDATORY YES OR NO DEFAULT: YES	no

Example

```
device set -n VSwitch1 -ip 212.199.43.46 -d 21/04/2002 -t 13:30 -c AnnaLevin. -loc ext4838 -if eth1 -rld no
```

device set -telnet

This command changes the Telnet port from the default port number to a user defined port number. Establishing a Telnet connection on an alternate port (not the expected port 23) provides increased line security.

```
device set -telnet
```

Example

```
device set -telnet 49155
```

fc interface show

This command shows each FC port and its World Wide Port Name (WWPN).

```
fc interface show
```

Alias	WWPN
fc2	20:00:00:20:38:00:10:64

fc node show

This command shows the V Switch World Wide Node Name (WWNN).

```
fc node show
```

Name	V Switch1
Description	SW Version 1.5, build 5,patch 0 Board version 1, PCB version
WWNN	20:00:20:10:58:00:10:46
Function	Gateway

fc set speed

This command allows you to set the speed of the FC communication.

```
fc set speed
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE	STORAGE PORT	MANDATORY	fc2
-sp	SPEED	FC COMMUNICATION SPEED	MANDATORY 1 GB: 1 2 GB: 2 DEFAULT: 1	1

interface show

This command shows the V Switch interfaces (ports) and their parameters.

```
interface show
```

Table 33: V Switch Interfaces

Type	Name	Description	Alias	Phys Address
RS232	cons	RS232 Management Int	cons	000000000000
ETHERNET	mgmt	Fast Ethernet Manage	mgmt	000000000000
FibreChannel	fc1	FC MMF	fc1	000000000000
FibreChannel	fc2	FC MMF	fc2	000000000000
FibreChannel	fc3	FC MMF	fc3	000000000000
FibreChannel	fc4	FC MMF	fc4	000000000000
FibreChannel	fc5	FC MMF	fc5	000000000000
FibreChannel	fc6	FC MMF	fc6	000000000000
ETHERNET	eth1	Gigabit Ethernet Net	eth1	00081a000110
ETHERNET	eth2	Gigabit Ethernet Net	eth2	00081a000111
ETHERNET	eth3	Gigabit Ethernet Net	eth3	00081a000112

interface details

This command lists the interface details of a specified interface.

```
interface details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE ALIAS	ALIAS OF INTERFACE TO SHOW	MANDATORY	eth1

Table 34: Interface Details

Parameter	Details
Name:	eth1
Alias:	eth1
Index:	9
Type:	ETHERNET
Description:	Gigabit Ethernet Network Interface
Phys Address:	0081a000110
MTU:	1500
Admin Status:	up
Oper. Status:	up

interface set

This command renames the specified interface alias.

```
interface set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE ALIAS OR NAME	CURRENT ALIAS OR NAME OF INTERFACE	MANDATORY	Storage1
-na	NEW ALIAS	NEW ALIAS OR NAME OF INTERFACE	OPTIONAL DEFAULT: DEFAULT INTERFACE NAMES – CONS, MGMT, FC1,ETH1	fc1

pscsi show

This command displays all parallel SCSI devices and their bus ID number.

```
pscsi show
```

Table 35: Parallel SCSI Device Bus IDs

Alias	BusID
p SCSI3	12
p SCSI4	7

pscsi set busid

This command assigns a bus ID to a parallel SCSI device.

```
pscsi set busid
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-if	INTERFACE	STORAGE PORT NUMBER/ALIAS	MANDATORY	p SCSI3
-id	ID	P SCSI ID NUMBER BETWEEN 0 AND 15	MANDATORY	12

Example

```
pscsi set busid if p SCSI3 -id 12
```

snmp manager show

This command displays the managers of the V Switch.

```
snmp manager show
```

Table 36: V Switch SNMP Managers

IP Address	Port	Read Community	Write Community	Trap
212.199.43.96	162	Public	Private	yes

snmp manager add

This command adds a manager to the V Switch.

```
snmp manager add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UPD PORT	PORT TO RECEIVE TRAPS THROUGH	OPTIONAL DEFAULT: 162	
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	
-trap	TRAP	TO SEND TRAPS TO MANAGER	OPTIONAL Y: SEND N: DO NOT SEND DEFAULT: Y	

snmp manager set

This command modifies parameters of existing managers.

snmp manager set

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UPD PORT	PORT TO RECEIVE TRAPS THROUGH	MANDATORY	150
-np	NEW PORT	NEW PORT FOR RECEIVING TRAPS	OPTIONAL	151
-rcom	READ COMMUNITY	COMMUNITY TO GET INFORMATION	OPTIONAL DEFAULT: PUBLIC	
-wcom	WRITE COMMUNITY	COMMUNITY TO SET INFORMATION	OPTIONAL DEFAULT: PRIVATE	
-trap	TRAP	TO SEND TRAPS TO MANAGER	OPTIONAL Y: SEND N: DO NOT SEND DEFAULT: Y	

snmp manager remove

This command removes a manager from the V Switch.

snmp manager remove

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	MANAGER IP ADDRESS	MANDATORY	212.199.43.96
-p	UPD PORT	PORT TO RECEIVE TRAPS THROUGH	MANDATORY	150

ip config show

This command displays the V Switch IP configurations.

```
ip config show
```

Table 37: V Switch IP Configurations

If Name	IP Address	Net Mask	Activity
mgmt	212.199.43.46	255.255.255.0	Active
eth1	212.199.43.56	255.255.255.0	Active
eth1	212.199.43.57	255.255.255.0	Inactive
eth2	212.199.75.66	255.255.255.0	Active
eth3	212.199.12.67	255.255.255.0	Inactive
eth3	212.199.12.70	255.255.255.0	Active

ip config set

This command configures a new interface alias or edits an existing one.

```
ip config set
```

Executing this command on the same network port with a different IP address will not reset the network port address. It will add another IP address to the network port

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS ASSIGNING TO THE INTERFACE PORT	MANDATORY	212.199.43.56
-if	INTERFACE ALIAS OR NAME	NETWORK INTERFACE PORT	MANDATORY ETH1, ETH2, ETH3	eth1
-im	IP MASK	IP NET MASK	OPTIONAL DEFAULT: 255.255.255.0	
-act	ACTIVITY	IF IP ADDRESS IS ACTIVE TO EXPOSE VOLUMES. USE INACTIVE STATUS TO ALLOW FAILOVER.	OPTIONAL DEFAULT: 1 (ACTIVE). 2(INACTIVE)	1

Example

```
ip config set -ip 212.199.43.56 -if eth1 -act 1
```

ip config remove

This command removes an IP address from an interface.

```
ip config remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
--------	-----------	------------	--------	---------

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-ip</code>	IP ADDRESS	IP ADDRESS TO REMOVE FROM THE NETWORK INTERFACE PORT	MANDATORY	<code>212.199.43.70</code>

Example

```
ip config remove -ip 212.199.43.70
```

ip route add

This command adds an IP route to a network port.

```
ip route add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-dip</code>	DESTINATION IP	IP OF HOST STATION	MANDATORY	<code>10.10.20.20</code>
<code>-dmask</code>	DESTINATION MASK	IP MASK OF HOST STATION	MANDATORY	<code>255.255.255.0</code>
<code>-gw</code>	GATEWAY IP ADDRESS	IP ADDRESS OF THE GATEWAY ROUTER	MANDATORY	<code>30.30.20.20</code>
<code>-if</code>	INTERFACE ALIAS	NETWORK PORT TO OPEN COMMUNICATION THROUGH	MANDATORY	<code>eth2</code>

Example:

An IP routing path to Network D, IP 10.10.20.20, (IP mask 255.255.255.0) is mapped from network port Eth2 through router gateway 30.30.20.20.

```
ip route add -dip 10.10.20.20 -dmask 255.255.255.0 -gw 30.30.20.20 -if eth2
```

ip route show

This command shows all IP routes on a V Switch.

```
ip route show
```

Dest IP Address	Dest Mask	Interface	Gateway
<code>10.10.20.20</code>	<code>255.255.255.0</code>	<code>Eth2</code>	<code>30.30.20.20</code>
<code>10.12.40.40</code>	<code>255.255.255.0</code>	<code>Eth3</code>	<code>20.22.11.11</code>

ip route remove

This command removes an IP route from a network port.

```
ip route remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
- dip	DESTINATION IP	IP OF HOST STATION	MANDATORY	10.12.40.40
- dmask	DESTINATION MASK	IP MASK OF HOST STATION	MANDATORY	255.255.255.0
- gw	GATEWAY	GATEWAY TO HOST STATION IP ADDRESS	MANDATORY	20.22.11.11
- if	INTERFACE ALIAS	NETWORK PORT TO OPEN COMMUNICATION THROUGH	MANDATORY	eth3

Example:

The routing path to destination network IP 10.12.40.40 (IP mask 255.255.255.0) is removed from network port Eth3.

```
ip route remove -dip 10.12.40.40 -dmask 255.255.255.0 -  
dmask 20.22.11.11 -if eth3
```

ip isns show

This command shows all iSNS servers configured on the V-Switch.

```
ip isns show
```

Table 38: iSNS Servers

```
212.199.43.2  
212.199.56.134
```

ip isns add

This command adds an iSNS server's IP address to the V-Switch iSNS client.

```
ip isns add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
- ip	IP ADDRESS	IP ADDRESS OF ISNS SERVER	MANDATORY	212.199.43.1

ip isns remove

This command removes an iSNS server's IP address from the V-Switch iSNS client.

```
ip isns remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF iSNS SERVER	MANDATORY	212.199.43.1

neighbor add

This command adds a neighbor to a cluster.

```
neighbor add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	VSwitch2
-ip	IP ADDRESS	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	212.199.43.75

Example

```
neighbor add -nb VSwitch2 -ip 212.199.43.75
```

neighbor set

This command resets a neighbor alias or IP address in a cluster.

```
neighbor set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	VSwitch2
-ip	IP ADDRESS	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	212.199.43.75

neighbor show

This command lists the neighbor(s) in a cluster.

```
neighbor show
```


Table 39: Neighbors in a Cluster

Name	IP Address	UDP	SNMP Timeout (msec)	SNMP # of Retries
VSwitch2	212.199.43.75	161	1500	3

neighbor details

This command lists the details of a neighbor in a cluster.

```
neighbor details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBOR IN CLUSTER	MANDATORY	VSwitch2

Table 40: Neighbor Details

Neighbor Name	VSwitch2
IP Address	212.199.43.75
Last Received Keep Alive:	3
Status	Alive
Lock Status	srOpen

neighbor remove

This command removes a V Switch from a cluster.

```
neighbor remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-nb	NEIGHBOR	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	VSwitch2

cluster show

This command shows the keep alive parameters of a cluster.

```
cluster show
```

Table 41: Cluster Table

Last Keep Alive:	1
KeepAlive Int(s):	2
Susp Int(s):	6

```

Last Keep Alive:      1
Dead Int(s):         10
Failover:             Enabled
State:                Running

```

cluster set

This command allows you to modify a cluster's parameters.

```
cluster set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-kai	KEEP ALIVE INTERVAL	TIME BETWEEN ALIVE SIGNALS FROM NEIGHBORS	MANDATORY IF CHANGING	5
-sint	SUSPICIOUS INTERVAL	TIME FROM WHEN A SIGNAL WAS EXPECTED BUT NOT RECEIVED	MANDATORY IF CHANGING	10
-fint	FAILOVER INTERVAL	TIME WHEN SUSPICIOUS INTERVAL IS EXCEEDED	MANDATORY IF CHANGING	20

Example:

The Keep Alive interval is set to 5 seconds. That is, every 5 seconds an alive signal is sent out to all neighboring V Switches. The neighboring V Switches register a suspicious interval after 10 seconds without an alive signal. This is the equivalent of 2 missed keep alive intervals. After a total of 20 seconds, from the first missed alive signal, the neighboring V Switches register a dead interval. This is the equivalent of 4 missed keep alive intervals.

```
cluster set -kai 5 -sint 10 -dint 20
```

cluster failover enable

This command enables the cluster failover functionality. This command must be executed on both V Switches in the cluster.

```
cluster failover enable
```

cluster failover disable

This command disables the cluster failover functionality. This command must be executed on both V Switches in the cluster.

```
cluster failover disable
```

ft show

This command displays the configuration for file transfer.

```
ft show
```

Table 42: File Transfer Configuration

Host IP:	212.199.43.46
File Name:	/usr/VSwitch/images/im1234.run
File Type:	af
Time Out	15
Number of Retries	3
Command	download
Status	Transferring
Error	ok

ft upload software

This command uploads a V Switch database file from the V Switch to the local TFTP server.

```
ft upload software
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	SERVER IP ADDRESS	MANDATORY	212.199.43.70
-fn	FILE NAME	NAME TO SAVE FILE AS	MANDATORY	Backupdata
-ft	FILE TYPE	FORMAT TO SAVE DATA IN	OPTIONAL DB – DATA BASE DEFAULT: DB	db

ft download

This command downloads a V Switch database configuration file from the local TFTP server.

```
ft download
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	212.199.43.70
-fn	FILE NAME	NAME TO SAVE FILE AS	MANDATORY	Backupdata

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ft	FILE TYPE	FORMAT TO SAVE DATA IN	OPTIONAL DB – DATA BASE	db
-tmo	TIME BEFORE TIMEOUT	NUMBER OF SECONDS BEFORE TIMEOUT	OPTIONAL 5 –3600 SEC	15
-nor	NUMBER OF RETRIES	NUMBER OF RETRIES TO CONNECT	OPTIONAL 0 – 10	3

ft export problem

This command exports three files: configuration file, last good database and the corrupted database file for examination.

You can only export after the V Switch reboots in safe mode.

`ft export problem`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	SERVER IP ADDRESS	MANDATORY	212.199.43.70
-fd	FILE DIRECTORY	DIRECTORY TO EXPORT FILES TO	MANDATORY	Backupdata

system boot

This command forces the V Switch to boot in Safe Mode.

`system boot`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-sm	SAFE MODE	SAFE MODE LEVEL	MANDATORY	1
			0: NORMAL 1: LAST GOOD CONFIGURATION 2: DEFAULT DATABASE 3: DEFAULT FACTORY SYSTEM	

system set

This command sets or unsets the system to work in database replication mode.

`system set`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-rep	REPLICATE	REPLICATION OF THE DATABASE	MANDATORY YES: REPLICATE NO: DO NOT REPLICATE	yes

system copy

This command copies the database from either the flash or compact flash to either the compact flash or flash.

`system copy`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-from	FROM	WHERE TO COPY FROM	MANDATORY FLASH CFLASH	cflash
-type	TYPE	TYPE OF FILE TO COPY	MANDATORY DB: DATABASE	db

system show

This command shows the status of both the compact flash and replication mode.

`system show`

```
Flash                present
Compact Flash       present
Database Configuration replicate
Database Current    replicate
```

Volume Configuration

These commands enable you to configure and view disks and volumes via the V Switch.

COMMAND	COMMAND
STORAGE DISCOVERY	VOLUME CREATE MIRROR
STORAGE BLINK ACTIVATE	VOLUME CREATE CONCATENATED
STORAGE BLINK ABORT	VOLUME CREATE STRIPED
STORAGE SHOW	VOLUME SET
STORAGE DISK SHOW	VOLUME REMOVE
STORAGE DISK SET	VOLUME REMOVE -ALL
STORAGE ALIAS	VOLUME REPLACE
STORAGE DETAILS	VOLUME MIRROR SHOW
STORAGE SET	VOLUME MIRROR SYNC
STORAGE REMOVE	VOLUME MIRROR DUMMYSYNC
SUBDISK CREATE	VOLUME COPY CREATE
SUBDISK SHOW	VOLUME COPY SHOW
SUBDISK DETAILS	VOLUME COPY ABORT
SUBDISK ALIAS	VOLUME MIRROR ADD
SUBDISK SET	VOLUME MIRROR BREAK
SUBDISK REMOVE	VOLUME RESIZE
VOLUME SHOW	VOLUME RETRACT
VOLUME DETAILS	VOLUME EXPAND
VOLUME ALIAS	VOLUME CREATE SNAPSHOT
VOLUME HIERARCHY	VOLUME SNAPSHOT SHOW
VOLUME CREATE SIMPLE	VOLUME SNAPSHOT LIST
VOLUME CREATE TRANSPARENT	

storage discovery

This command resets the Fiber Channel loop and reregisters all attached storage devices. This command is used after adding or removing storage devices from the V Switch topography. Because this command resets the FC loop, it will cause a failure of any I/O operations being executed when the command is invoked.

```
storage discovery
```

storage blink activate

This command allows you to blink a storage device to identify it.

```
storage blink activate
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE DEVICE	ALIAS OF DEVICE TO BLINK	MANDATORY	Stor_1
-t	TIME	LENGTH OF TIME TO BLINK DEVICE	MANDATORY 1-3600 SEC 0=FOREVER	120

storage blink abort

This command stops a storage device from blinking.

```
storage blink abort
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE DEVICE	ALIAS OF DEVICE TO BLINK	MANDATORY	Stor_1

storage show

This command shows all storage devices connected to the V Switch.

```
storage show
```

Table 43: Storage Devices

Alias	Entity Name	LUN	Oper. Status	Type
Stor_1	0102030405060708	0	Disabled	disk
Stor_2	090a0b0c0d0e0f10	0	Enabled	entire
Stor_3	090a0b0c0d0e0f10	1	Enabled	split

Alias	Entity Name	LUN	Oper. Status	Type
disk4	0102030405060708	0	Storage is missing	entire

storage disk show

This command shows all storage disks connected to the V Switch.

```
storage disk show
```

Table 44: Storage Disks

Alias	Entity Name	LUN	Oper. Status	Subdisk
disk1	01:02:03:04:05:06:07:08	0	Disabled	entire
disk2	09:0a:0b:0c:0d:0e:0f:10	0	Enabled	entire
disk3	09:0a:0b:0c:0d:0e:0f:10	1	Enabled	split
disk4	01:02:03:04:05:06:07:08	0	Storage is missing	entire

storage disk set

This command allows you to enable or disable write cache for a disk.

```
storage disk set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-d	DISK	DISK DEVICE	MANDATORY	Disk2JBOD5
-wce	WRITE CACHE ENABLED	WRITE CACHE FUNCTION	MANDATORY YES OR NO	yes

storage alias

This command allows you to view all storage aliases in full. The command **storage show** has a ten-character display limit so storage aliases may be ambiguous in the storage show table.

```
storage alias
```

Table 45: Storage Aliases

Entity Name	LUN	Alias
2000002037d8e314	000	Stor_1
2000002037f8ba50	000	Stor_2

storage details

This command shows all storage devices attached to the V Switch.

```
storage details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE ALIAS	ALIAS OF STORAGE TO VIEW	MANDATORY	disk1

Table 46: Storage Details

```
Alias: Disk2JBOD5
Entity Name: 2000002037a9551e
LUN(Logical Unit Number) 0000000000000000
Vendor Name: SEAGATE
Additional Info:
Transport type: Fiber Channel
Oper. Status: Enabled
Time since last Update: 8 days 3h:12m:16 sec 37
(1/60 Sec)
SCSI Version: 3
Revision Level: 0002ST336704FC
Product Id: ST336704FC
Serial Number: 3CD0FHA400002108XYGLXYGL
Number Of Blocks: 71687369
Block Size: 512
SubDisks: Entire
Write Cache Enabled: true
Write Protected false
Volume sim
```

storage set

This command allows you to edit storage device parameters.

```
storage set
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE ALIAS	STORAGE ALIAS TO MODIFY	MANDATORY	Stor_7
-na	NEW ALIAS	NEW ALIAS FOR STORAGE	MANDATORY IF CHANGING	disk7
-info	INFORMATION	INFORMATION ON STORAGE TO SET	MANDATORY IF CHANGING	replace_disk2

storage remove

This command removes a storage device from the database only if the storage device state is defined as *StorageIsMissing*.

storage remove

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-s	STORAGE	ALIAS OF STORAGE TO REMOVE	MANDATORY	Stor_1

subdisk create

This command creates a subdisk according to the input parameters.

subdisk create

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-d	DISK ALIAS	ALIAS OF DISK IN WHICH TO CREATE THE SUBDISK	MANDATORY	Disk 1
-sl	SUBDISK LENGTH	LENGTH IN BLOCKS OF SUBDISK	MANDATORY	18000000
-sa	START ADDRESS	BLOCK ADDRESS TO BEGIN CREATING SUBDISK FROM	OPTIONAL DEFAULT: 0	0
-sd	SUBDISK ALIAS	ALIAS FOR NEW SUBDISK	OPTIONAL DEFAULT FORMAT: DEF_ SPLIT_CLUSTER NO._DISK NO._ END ADDRESS	Subdisk 1

subdisk show

This command shows all/specified subdisks connected to the V Switch.

`subdisk show`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-d</code>	DISK ALIAS	ALIAS OF DISK TO SHOW SUBDISKS FROM	OPTIONAL USE THIS SWITCH TO LIST ONLY THE DETAILS OF A SPECIFIC DISK	

Table 47: Details of all Subdisks

Disk	Subdisk	Start Address	Length	Vol
<code>disk1</code>	<code>split1</code>	0	512	<code>yes</code>
<code>disk1</code>	<code>split2</code>	512	512	<code>yes</code>
<code>disk2</code>	<code>split1</code>	0	2048	<code>no</code>
<code>disk2</code>	<code>split2</code>	2048	512	<code>yes</code>
<code>disk3</code>	<code>split1di*~</code>	0	1024	<code>no</code>
<code>disk3</code>	<code>split2</code>	1024	1024	<code>no</code>

subdisk details

This command shows all/specified subdisks on a disk.

`subdisks details`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-d</code>	DISK ALIAS	ALIAS OF DISK TO SHOW SUBDISKS ON	MANDATORY	<code>disk1</code>
<code>-sd</code>	SUBDISK ALIAS	ALIAS OF SUBDISK TO SHOW	OPTIONAL	

Table 48: Details of a Specified Subdisk

Subdisk	Start Address	Length	Allocated	volume	Details	Last Update
<code>split1</code>	0	512	<code>yes</code>	<code>vsplit2</code>	<code>" "</code>	11/11/01 12:30
<code>split2</code>	512	512	<code>yes</code>	<code>split 3</code>	<code>" "</code>	11/11/01 12:30

subdisk alias

This command allows you to view all subdisk aliases in full. The command `subdisk show` has a ten-character display limit so subdisk aliases may be ambiguous in the subdisk show table.

`subdisk alias`

Table 49: Subdisk Aliases

Disk	Length	Alias
Disk3	1024	split1disk3
Disk7	1024	split1disk7
Disk7	1024	split2mirror

subdisk set

This command renames a subdisk and allows you to edit the subdisk information.

`subdisk set`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-sd</code>	SUBDISK ALIAS	ALIAS OF SUBDISK TO RENAME	MANDATORY	<code>sub1</code>
<code>-na</code>	NEW SUBDISK ALIAS	NEW ALIAS OF SUBDISK	MANDATORY IF CHANGING THE ALIAS	<code>mir1</code>
<code>-info</code>	INFORMATION	INFORMATION ON SUBDISK FOR LOCAL ADMINISTRATION ONLY	MANDATORY IF CHANGING	

subdisk remove

This command removes a specified subdisk.

`subdisk remove`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
<code>-sd</code>	SUBDISK ALIAS	ALIAS OF SUBDISK TO DELETE	MANDATORY	<code>sub1</code>

volume show

This command shows all volumes defined in the database.

`volume show`

Table 50: Volume Details of all Volumes

Alias	Type	Act # of Bl	Pot # of Bl	Bl Size	State
Simple1	Simple	17999999	17999999	512	Internal
RLU1	Simple	17999999	17999999	512	Exposed
Mir1	Mirror	8388608	8388608	512	Exposed
RLU3	Simple	16777216	16777216	512	Internal

volume details

This command shows all details of a specified volume.

volume details

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF SINGLE VOLUME DETAILS TO SHOW	MANDATORY	stripe1

Table 51: Specific Volume Details

Alias	Snp3Stripe1
Type	stripe
Number of Blocks	41943040
Actual Size	25 GB
Potential Size	50 GB
Block Size	512
State	internal
Stripe Size	200
Snapshot of	Stripe1
Created	Mon. 15 Dec. 2003 01:13
Threshold	80%
Percentage Utilized	90%
# of SubVolumes	-
Parent	RAID
Time Since Last Reset	1 days 4h:14m:21s
Child	voll

Alias	Snp3Stripe1
Child	vol2

volume alias

This command allows you to view all volume aliases in full. The command **volume show** has a ten-character display limit so volume aliases may be ambiguous in the volume show table.

```
volume alias
```

Table 52: Volume Aliases

Volume Type	Alias
striped	MusicBoxTop40
concat	Entertainment
mirrored	Oct02PayRoll

volume hierarchy

This command shows the volumes composing the specified volume.

```
volume hierarchy
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO DISPLAY	MANDATORY	stripe1

Table 53: Volume Hierarchy

Alias	Type	#SubVolume	Parent	State
stripe1	striped	2	RAID	internal
vol1	simple	0	stripe1	internal
vol2	simple	0	stripe1	internal

volume create simple

This command creates a simple volume out of a disk or subdisk.

```
volume create simple
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF SIMPLE VOLUME	OPTIONAL DEFAULT: (SUB)DISK ALIAS	

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-sd	SUBDISK ALIAS	ALIAS OF SUBDISK TO USE	MANDATORY IF USING A SUBDISK	
-d	DISK	ALIAS OF DISK TO USE	MANDATORY IF USING A DISK	

volume create transparent

This command creates a transparent volume out of a disk.

`volume create transparent`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO CREATE	OPTIONAL DEFAULT: DISK ALIAS	trans1
-d	DISK	ALIAS OF DISK TO USE	MANDATORY	Stor_3

volume create mirror

This command creates a mirrored volume the specified number of volumes.

`volume create mirror`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO CREATE	MANDATORY	Mirror2
-nbc	NUMBER OF CHILDREN	NUMBER OF VOLUMES IN MIRROR	OPTIONAL FROM 2 TO 4 DEFAULT: 2	2
-ch	CHILD	ALIAS OF EACH VOLUME TO INCLUDE IN MIRROR	MANDATORY	Simple1
-ch	CHILD	ALIAS OF EACH VOLUME TO INCLUDE IN MIRROR	MANDATORY	Simple2

volume create concatenated

This command creates a concatenated volume across the specified volumes in the order listed.

`volume create concatenated`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO CREATE	MANDATORY	Concat1
-nbc	NUMBER OF CHILDREN	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL DEFAULT: 2	2
-ch	CHILD	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY	Simple1
-ch	CHILD	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY	Simple2

volume create striped

This command creates a striped volume across the specified volumes in the order listed.

volume create striped

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME	MANDATORY	Stripe1
-sus	STRIPED UNIT SIZE	NUMBER OF BLOCKS TO WRITE IN EACH VOLUME PER PASS	MANDATORY	200
-nbc	NUMBER OF CHILDREN	NUMBER OF VOLUMES TO CREATE STRIPE ACROSS	OPTIONAL DEFAULT: 2	2
-ch	CHILD	ALIAS OF EACH VOLUME IN STRIPE	MANDATORY	Simple3
-ch	CHILD	ALIAS OF EACH VOLUME TO INCLUDE IN MIRROR	MANDATORY	Simple4

volume set

This command will change a volume alias or load threshold.

volume set

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO CHANGE	MANDATORY	Subdisk7
-na	NEW ALIAS	NEW ALIAS FOR VOLUME	MANDATORY IF CHANGING ALIAS	Simple7
-lt	LOAD THRESHOLD	PERCENTAGE FULL AT DESTINATION TO TRIGGER AN ALARM	MANDATORY IF CHANGING LOAD THRESHOLD	70

volume remove

This command removes a volume from the system. The volume must be at the top of the hierarchy. The volume cannot be exposed; the volume LU must be inactivated.

volume remove

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO REMOVE	MANDATORY	Stripe3

volume remove -all

This command removes a volume and **all volumes composing it** in the hierarchy. The volume must be at the top of the hierarchy. The volume cannot be exposed; the volume LU must be inactivated. Simple volumes will convert back to their component disks or subdisks.

volume remove -all

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME ALIAS	ALIAS OF TOP-LEVEL VOLUME TO REMOVE	MANDATORY	Stripe 1

volume replace

This command replaces a volume with another volume. Use this command after a disk failure to replace a volume used in a storage hierarchy with a volume on a functional disk.

If you are replacing a volume used as part of a mirrored volume, use the CLI command **volume mirror-synch** to synchronize the replacement volume with the other mirrored volume(s). See the working example: "Replacing a Mirrored Volume," page 256.

volume replace

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME ON FAILED DISK	MANDATORY	Simple4
-nvol	NEW VOLUME	REPLACEMENT VOLUME	MANDATORY	Simple6

volume mirror show

This command shows the status of all synchronized mirrored volumes in the V Switch.

volume mirror show

Volume Alias	Source Alias	Operational Status	Progress
Mirror8	Mirror2	Synchronizing	60%
Mirror4	Mirror3	Last sync succeeded	100%
Mirror 12	Mirror10	none	-

volume mirror sync

This command synchronizes mirrored volumes. Use this command after adding another volume to a group of mirrored volumes or to restore a mirrored volume on a disk after a disk failure.

volume mirror sync

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	Mirror2
-dst	DESTINATION	ALIAS OF VOLUME TO COPY TO	MANDATORY	Mirror8

volume mirror dummysync

This command performs a dummy synchronization on the non-exposing V Switch in a cluster after the mirrored volumes have been synchronized on the exposing V Switch.

volume mirror dummysync

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
--------	-----------	------------	--------	---------

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	Mirror2
-dst	DESTINATION	ALIAS OF VOLUME TO COPY TO	MANDATORY	Mirror8

volume copy create

This command creates an off-line volume copy.

`volume copy create`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	ScienceLab
-dst	DESTINATION	ALIAS OF VOLUME TO COPY TO	MANDATORY	ScienceLabII

volume copy show

This command shows all on-going and previously executed operations on volumes

`volume copy show`

Volume Alias	Source Alias	Operational Status	Progress
Mirror8	Mirror2	Synchronizing	60%
Mirror4	Mirror3	Last sync succeeded	100%

volume copy abort

This command aborts an off-line volume copy operation.

`volume copy abort`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	ALIAS OF SOURCE VOLUME TO COPY	MANDATORY	ScienceLab
-dst	DESTINATION	ALIAS OF VOLUME TO ABORT COPY TO	MANDATORY	ScienceLabII

volume mirror add

This command adds an on-line volume copy to a mirror or the head of a hierarchy.

```
volume mirror add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	SOURCE VOLUME TO ADD MIRROR TO	MANDATORY	Mirror5
-ch	CHILD	NEW CHILD TO ADD TO MIRROR	MANDATORY	Simple10
-dst	DESTINATION	ALIAS OF NEW MIRROR	OPTIONAL	Mirror5a
-no sync	NO SYNCHRONIZATION	DISABLE AUTOMATIC MIRROR SYNC	OPTIONAL NO SYNCIF USED	-nosync

volume mirror break

This command removes a child from a mirror volume.

```
volume mirror break
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME MIRROR IS ADDING TO	MANDATORY	Mirror5
-ch	CHILD	CHILD TO BREAK FROM MIRROR	MANDATORY	Simple10

volume resize

This command increases a volume's potential capacity on-line.

```
volume resize
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	VOLUME TO RESIZE	MANDATORY	
-dst	DESTINATION	ALIAS OF RESIZED VOLUME	OPTIONAL	

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-with	SIMPLE VOLUME	VOLUME TO RESIZE WITH	MANDATORY	

volume retract

This command retracts a volume by deleting all added volumes use to resize the volume. This command only works if the resized volume has not been expanded. The head of the volume hierarchy is retracted, not the resized volume.

`volume retract`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME TO RETRACT – HEAD OF HIERARCHY	MANDATORY	Mir5

volume expand

This command expands a volume's actual capacity to match its potential capacity.

`volume expand`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	VOLUME TO EXPAND	MANDATORY	Simple3

volume create snapshot

This command creates a snapshot

`volume create snapshot`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-src	SOURCE	SOURCE OF SNAPSHOT	MANDATORY	Mirror3
-dst	DESTINATION	SNAPSHOT DESTINATION	MANDATORY	Snp1Mir3
-lt	LOAD THRESHOLD	PERCENTAGE FULL AT DESTINATION TO TRIGGER AN ALARM	OPTIONAL DEFAULT: 80%	50

volume snapshot show

This command shows all source volumes and their snapshot volumes.

```
volume snapshot show
```

Source	Snapshot	Date & Time	Utilization
Mirror3	Snp1Mir3	11/01/04 8:34:28	60%
Mirror2	Snp7Mir2	09/01/04 15:53:07	100%

volume snapshot list

This command shows all snapshot volumes for a specific source volume.

```
volume snapshot list
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	SNAPSHOT SOURCE VOLUME	MANDATORY	Mirro2

Volume Exposure

These commands enable you to expose volumes using iSCSI protocol to network hosts and control access the exposed volumes.

COMMAND	COMMAND
ISCSI PORTAL SHOW	ACL IDENTITY ADD NAME
ISCSI PORTAL CREATE	ACL IDENTITY REMOVE NAME
ISCSI PORTAL REMOVE	ACL IDENTITY ADD CHAP
ISCSI TARGET SHOW	ACL IDENTITY REMOVE CHAP
ISCSI TARGET CREATE	ACL IDENTITY ADD SRP
ISCSI TARGET ALIAS	ACL IDENTITY REMOVE SRP
ISCSI TARGET SET	ACL IDENTITY SET
ISCSI TARGET REMOVE	ACL UP
ISCSI TARGET AUTHENTICATION	ACL DOWN
ACL SHOW	IP RADIUS SHOW
ACL DETAILS	IP RADIUS ADD
ACL ADD	IP RADIUS SET
ACL SET	IP RADIUS REMOVE
ACL REM	VOLUME EXPOSE –NEW
ACL IDENTITY SHOW	VOLUME EXPOSE
ACL IDENTITY DETAILS	LU SHOW
ACL IDENTITY CREATE	LU DETAILS
ACL IDENTITY DELETE	LU REMOVE

iscsi portal show

This command shows the portals defined for iSCSI on the V Switch with which you are communicating.

```
iscsi portal show
```

Table 54: iSCSI Portals

Protocol	Address Type	Address	Port
6	IPv4	172.17.200.156	5003
6	IPv4	172.17.200.150	5003

iscsi portal create

This command creates an iSCSI portal on a 1 Gb (network) port.

```
iscsi portal create
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF NETWORK PORT	MANDATORY	212.199.43.70
-p	TCP PORT	TCP PORT FOR iSCSI COMMUNICATION	OPTIONAL DEFAULT: 3260	5003

iscsi portal remove

This command removes an iSCSI portal on a 1 Gb (network) port.

```
iscsi portal remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF NETWORK PORT	MANDATORY	212.199.43.70
-p	TCP PORT	TCP PORT FOR iSCSI COMMUNICATION	OPTIONAL DEFAULT: 3260	5003

iscsi target show

This command shows all created targets.

```
iscsi target show
```


Table 55: iSCSI Targets

Target Alias	Target Name	# of LU	Exposed On:
wind	wwui	1	VSwitch1
fire	wwui	2	VSwitch2
water	wwui	1	VSwitch1
Presiden*~	wwui	1	VSwitch2
Presiden*~	wwui	1	VSwitch2

iscsi target create

This command creates an iSCSI target without creating LU0, attaching volumes or exposing the target. Targets can be created in advance and only later have LUNs created and exposed.

```
iscsi target create
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	USER-ASSIGNED ALIAS FOR ISCSI TARGET	MANDATORY	Finance
-tn	TARGET WWUI	USER-ASSIGNED WORLD-WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY	billing.sanrad
-device	DEVICE	ALIAS OF V SWITCH TO EXPOSE TARGET ON	MANDATORY	VSwitch1

iscsi target alias

This command allows you to view all subdisk aliases in full. The command **iscsi target show** has a ten-character display limit so iscsi target aliases may be ambiguous in the iscsi target show table.

```
iscsi target alias
```

Table 56: iSCSI Target Aliases

Target Name	Target Alias
wwui	PresidentPersonal
wwui	PresidentPublic
wwui	BillingRecords

iscsi target set

This command renames a target alias.

iscsi target set

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF TARGET TO RENAME	MANDATORY	Pilote
-n	NEW ALIAS	NEW ALIAS FOR TARGET	MANDATORY	Buffy

iscsi target remove

This command removes an iSCSI target.

iscsi target remove

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET TO REMOVE	MANDATORY	MusicBox

iscsi target authentication

This command allows the assigning of a password to a target to allow CHAP authentication at initiator connection to the target.

iscsi target authentication

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET TO REMOVE	MANDATORY	MusicBox
-pw	PASSWORD	PASSWORD OF TARGET	OPTIONAL DEFAULT: SANRADSANRAD	
-un	USER NAME	USER NAME OF TARGET	OPTIONAL DEFAULT: SANRAD	

acl show

This command shows all target access per identity for the V Switch.

acl show

Table 57: Target Access per Identity

Target	Position	Identity	Access
Finance	0	DEF_ALL	not-accessible

Target	Position	Identity	Access
Finance	1	Identity5	read-only
Finance	2	Identity2	read-write
SQL	0	DEF_ALL	not-accessible
SQL	1	Identity7	read-write
Library	0	DEF_ALL	not-accessible
Library	1	Identity4	read-only
Library	2	Identity7	read-write

acl details

This command shows the access control for a target.

```
acl details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET	MANDATORY	disk1

Table 58: Access Control per Target

Target	Position	Identity	Access
disk1	1	Identity5	read-only
disk1	2	Identity3	read-only
disk1	3	Identity1	read-write

acl add

This command links an identity and a target.

```
acl add
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET	MANDATORY	water
-id	IDENTITY	NAME OF ACL	MANDATORY	health_club
-acc	ACCESS RIGHTS	ACCESS RIGHTS TO THE TARGET	OPTIONAL OPTIONS: RW, RO OR NA DEFAULT: RW	rw

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-pos	POSITION	ACCESS PRIORITY LEVEL	OPTIONAL DEFAULT: 1	1

acl set

This command changes the access rights of an existing identity as it is linked with a specific target.

`acl set`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET	MANDATORY	water
-id	IDENTITY	NAME OF ACL	MANDATORY	health_club
-acc	ACCESS RIGHTS	ACCESS RIGHTS TO THE TARGET	OPTIONAL MANDATORY IF CHANGING	ro
-pos	POSITION	ACCESS PRIORITY LEVEL	OPTIONAL MANDATORY IF CHANGING	3

acl rem

This command removes an identity from the access control list of a specific target.

`acl rem`

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF ISCSI TARGET	MANDATORY	water
-id	IDENTITY	NAME OF ACL	MANDATORY	health_club

acl identity show

This command lists the identities in a V Switch.

`acl identity show`

Table 59: iSCSI Initiators in an Identity

Alias	Definition
-------	------------

Alias	Definition
health_club	members
library_staff	all library employees

acl identity details

This command lists the details of a specific identity.

```
acl identity details
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Library

Table 60: Identity Details

Description:	All library employees
Initiators:	iqn.com.ibm.Chandler iqn.com.cisco.Nigel iqn.com.ibm.Helen iqn.com.cisco.Julia
Credentials:	CHAP

acl identity create

This command creates a new identity for the V Switch.

```
acl identity create
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-info	INFORMATION	INFORMATION ON IDENTITY	OPTIONAL	All_registered_students

acl identity delete

This command deletes an identity from the V Switch.

```
acl identity delete
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School

acl identity add name

This command adds an iSCSI initiator to an identity.

```
acl identity add name
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-name	INITIATOR NAME	WWUI OF INITIATOR	MANDATORY	iqn.com.ibm.Sarah

acl identity remove name

This command removes an iSCSI initiator from an identity.

```
acl identity remove name
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-name	INITIATOR NAME	WWUI OF INITIATOR	MANDATORY	iqn.com.ibm.Buffy

acl identity add chap

This command adds CHAP authentication credentials to an identity.

```
acl identity add chap
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-un	USER NAME	HOST NAME	MANDATORY	Sarah

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-pw	USER PASSWORD	HOST PASSWORD	MANDATORY WITHOUT RADIUS 12 – 16 PRINTABLE CHARACTERS OPTIONAL WITH RADIUS	scalpelblades
-radius	RADIUS SERVER	USE RADIUS SERVER	OPTIONAL YES OR NO DEFAULT: NO	no

acl identity remove chap

This command removes a CHAP authentication credential from an identity.

```
acl identity remove chap
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-un	USER NAME	HOST NAME	MANDATORY	Sarah

acl identity add srp

This command adds SRP authentication credentials to an identity.

```
acl identity add srp
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-un	USER NAME	HOST NAME	MANDATORY	Robert
-pw	USER PASSWORD	HOST PASSWORD	MANDATORY	cardiac

acl identity remove srp

This command removes an SRP authentication credential from an identity.

```
acl identity remove srp
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
--------	-----------	------------	--------	---------

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-un	USER NAME	HOST NAME	MANDATORY	Robert

acl identity set

This command allows changes to an identity.

acl identity set

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-na	NEW ALAIS	NEW ALAIS FOR IDENTITY	OPTIONAL	Medschool
-info	INFORMATION	INFORMATION ON IDENTITY	OPTIONAL	all_students
-radius	RADIUS SERVER	RADIUS AUTHENTICATION USED	OPTIONAL YES OR NO	yes

acl up

This command pushes an identity position up in priority.

acl up

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET	TARGET ALAIS	MANDATORY	sql
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-n	JUMP SIZE	NUMBER OF PLACES TO MOVE UP	OPTIONAL DEFAULT: 1	

acl down

This command pushes an identity position down in priority.

acl down

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET	TARGET ALAIS	MANDATORY	sql
-id	IDENTITY	NAME OF ACL	MANDATORY	Med_School
-n	JUMP SIZE	NUMBER OF PLACES TO MOVE DOWN	OPTIONAL DEFAULT: 1	2

ip radius show

This command shows all IP addresses for RADIUS servers configured on the V Switch RADIUS client.

Table 61: RADIUS Server IP Addresses

```
212.199.43.2
212.199.56.134
```

ip radius add

This command adds a RADIUS server IP address to the V Switch RADIUS client.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF RADIUS SERVER	MANDATORY	212.199.43.2
-p	PORT	PORT NUMBER	OPTIONAL	24562
-key	KEY	SHARED SECRET BETWEEN V-SWITCH AND RADIUS SERVER	OPTIONAL	DataMakesMeHot

ip radius set

This command allows changes to a RADIUS server configuration on the V Switch RADIUS client.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF RADIUS SERVER	MANDATORY	212.199.43.2
-p	PORT	PORT NUMBER	OPTIONAL	

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-key	KEY	SHARED SECRET BETWEEN V-SWITCH AND RADIUS SERV	OPTIONAL	Xqjz1m7s9rjb

ip radius remove

This command removes a RADIUS server IP address from the V Switch RADIUS client.

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ip	IP ADDRESS	IP ADDRESS OF RADIUS SERVER	MANDATORY	212.199.43.2
-p	PORT	PORT NUMBER	OPTIONAL	

volume expose -new

This command creates a new LU0 and a new target for a specified volume.

volume expose -new

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME ALIAS	ALIAS OF VOLUME TO CREATE LU0 AND TARGET FOR	MANDATORY	Concat 1
-ta	TARGET ALIAS	USER-ASSIGNED ALIAS OF TARGET TO CREATE	MANDATORY ALIAS CANNOT CONTAIN SPACES	MusicBox
-tn	TARGET WWUI	USER-ASSIGNED WORLD WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY	Ourcompany.com/SAN/MusicBox
-device	DEVICE	ALIAS OF V SWITCH TO EXPOSE TARGET ON	MANDATORY	V Switch 1

volume expose

This command creates a new LU0 for a specified volume and exposes it on an existing target.

volume expose

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
--------	-----------	------------	--------	---------

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-vol	VOLUME	ALIAS OF VOLUME TO CREATE LU0 AND TARGET FOR	MANDATORY	Stripe1
-ta	TARGET ALIAS	ALIAS OF NEW TARGET TO CREATE	MANDATORY	music.sanrad
-lun	LOGICAL UNIT NUMBER	NUMBER TO ASSIGN TO VOLUME FOR EXPOSURE	MANDATORY	0
-p	PROTOCOL	EXPOSING PROTOCOL	OPTIONAL DEFAULT: iSCSI	iscsi

lu show

This command shows all LUNs defined in the database.

```
lu show
```

Table 62: Details of all LUNs

LUN	Tgt Alias	Volume	Oper Status
0	Pilote	xxx	Active
0	Spirou	yyy	Active
1	Pilote	Mir1	Active
0	1	zzz	Active

lu details

This command shows the details of an LU in the database.

lu details

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET	ALIAS OF TARGET OF LUN	MANDATORY	Spirou
-lun	LOGICAL UNIT NUMBER	LUN TO SHOW	MANDATORY	1

Example:

```
lu details -ta Spirou -lun 1
```

Table 63: LUN Details

Target Alias	Spirou
Target Type	iSCSI
LUN	1
Volume	Mir1
Status	active
Virtual Last Reset	3 days:12 h: 7m: 2sec

lu remove

If you remove LU0 you will disable the associated target even if the target has other attached LUs

This command removes the LU from its target. The LU must be inactive before being removed. This command is the opposite of **volume expose**.

```
lu remove
```

SWITCH	PARAMETER	DEFINITION	STATUS	EXAMPLE
-ta	TARGET ALIAS	ALIAS OF TARGET TO REMOVE LU FROM	MANDATORY	Pilote
-lun	LOGICAL UNIT NUMBER	LU TO REMOVE FROM THE TARGET	MANDATORY	0

User Notes



A

Sample Configurations

IN THIS CHAPTER

SAMPLE
INTRODUCTION

INSTALLING AND
USING THE V-SWITCH
3000

REPLACING A
MIRRORED VOLUME

REPLICATING DATA
OFF-LINE

CONFIGURING THE V-
SWITCH WITH A
SINGLE IP ROUTING
PATH

CONFIGURING A
CLUSTER

This chapter details working examples of how to install, configure and use the V-Switch with a Microsoft iSCSI initiator on a Windows™ 2000 platform for:

- ❑ Basic V-Switch configuration with volume creation and exposure.
- ❑ Individual disk replacement and mirrored volume reconstitution.
- ❑ Off-line data replication.
- ❑ IP routing path configuration.
- ❑ Basic cluster configuration.

Sample Introduction

This chapter provides working examples of standard procedures and configurations you will use in owning and operating your V-Switch.

Each example uses one basic storage network consisting of:

- One JBOD appliance with four disks of equal capacity (the actual capacity is not important) connected to the V-Switch.
- A PC running on the Windows™ 2000 OS platform.
- Microsoft iSCSI initiator software installed on each host terminal.
- Pre-assigned IP addresses for host and management stations.

Installing and Using the V-Switch 3000

You have just purchased a V-Switch 3000 and want to begin managing your company's small but growing storage network.

So far you have:

- One JBOD appliance with four disks of equal capacity (the actual capacity is not important) connected to the 3000.
- One PC acting as both management station for the 3000 and network host station for the storage network. The management station function is connected to the 3000 via an RS232 cable. The network host function is connected to the 3000 via a 1 Gbit Ethernet RJ45 cable.
- An IP address assigned to the management/host station.

In this example, the network port IP address will be assigned 172.17.200.174 and the iSCSI portal for network port Eth1 will be set to 5003.

This example explains how to:

- Use one terminal as both a management and host station.
- Initialize and manage the 3000 through an RS232 connection and terminal emulation program.
- Create a RAID 10 volume and expose it.
- Configure your iSCSI initiator for access to the exposed volume.

Once you have your components organized, you can begin.

STEP 1. ATTACH CABLES

Attach an HSSDC-DB9 fibre channel cable from your JBOD appliance to one of the storage ports on the back panel of the V-Switch. See #1, Figure 98, page 250. Depending on your appliance, you need to plug a terminator into one of the JBOD ports.

Attach the included RS232 cable from your management/host station to the console port (**Console**) on the back panel of the V-Switch. See #2, Figure 98, page 250.

Attach an RJ45 copper 1 Gbit Ethernet cable to the Ethernet port **Eth1** on the front panel of the V-Switch. See #3, Figure 98, page 250.

Your network should mimic Figure 98, page 250.

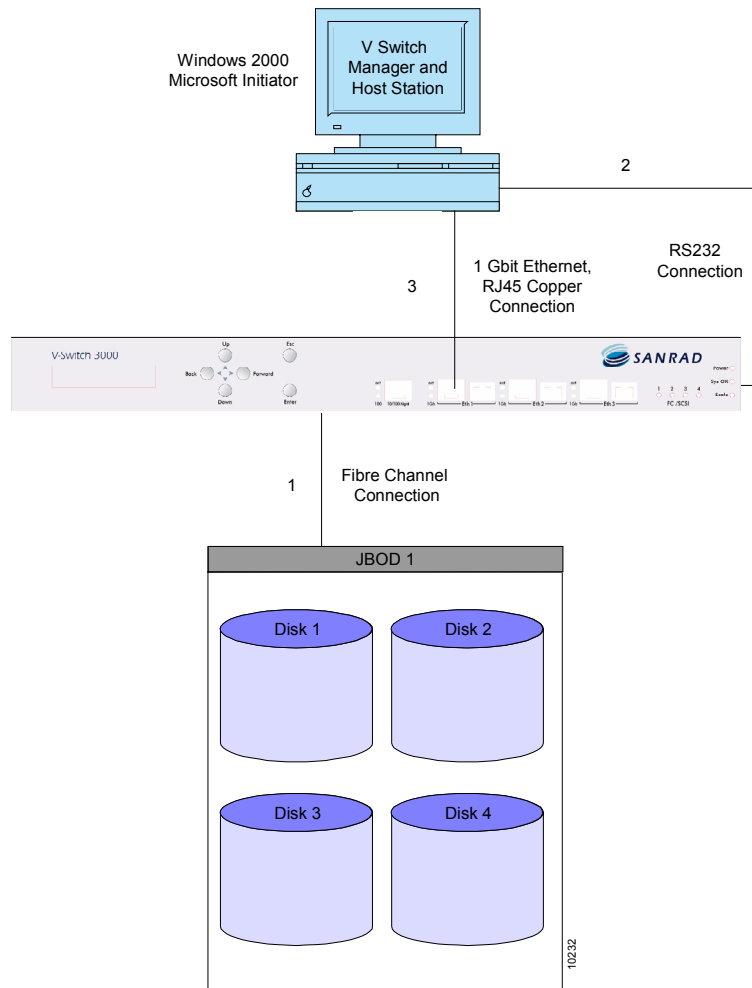


Figure 98. System Overview

STEP 2. POWER UP STORAGE DEVICE

Power up the JBOD appliance first to allow the V-Switch to register it in its network scan.

STEP 3. POWER UP V-SWITCH

Connect the power cord to the V-Switch and then to the electric socket. Turn the V-Switch on. The V-Switch powers up. The fan assembly is running and the LCD panel displays:

```
V-Switch 3000
Status: OK
```

STEP 4. CONFIGURE CONSOLE

You are using your PC as both the V-Switch's management station and the network host station.

Before you can open a CLI session via the RS232 connection, your console must be configured to allow communication between the two devices.

Open your terminal emulation program and set the system parameters as follows:

Table 64: Console Configuration Parameters

PARAMETER	SYSTEM REQUIREMENT
CONFIG SERIAL PORT	COM
BITS PER SECOND	115200
DATA BITS	8
PARITY	NONE
STOP BITS	1
FLOW CONTROL	NONE

STEP 5. LOGIN TO THE MANAGEMENT PORT

From the open terminal emulation window, press **Enter** on your keyboard to open the **V-Switch 3000 Login** window.



Figure 99. V-Switch 3000 Login Window

Enter the default user name, **sanrad**, and password, **sanrad**, and press **Enter** on your keyboard. The CLI prompt **>** appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

STEP 6. INITIALIZE V-SWITCH

From the open terminal emulation window, use the CLI command **init** to name the V-Switch.

```
init -n VSwitch1
```

Use the CLI command **ip config set** to assign an IP address to the network port Eth 1. Configure the port as active (**1**) to allow active communications through the port.

```
ip config set -ip 172.17.200.174 -if eth1 -im  
255.255.255.0 -act 1
```

STEP 7. CONFIGURE ISCSI PORTAL

The port number you set in the CLI must coincide with the port number you set in your iSCSI initiator configuration.

Use the CLI command `iscsi portal create` to configure the iSCSI portal on network port Eth 1 for iSCSI communications between the V-Switch and the host station.

```
iscsi portal create -ip 172.17.200.174 -p 3260
```

Use the CLI command `iscsi portal show` to view the created iSCSI portal.

```
iscsi portal show
```

Table 65: iSCSI Portal

Protocol	Address Type	Address	Port
6	IPv4	172.17.200.174	3260

STEP 8. CHECK STORAGE DEVICES

Use the CLI command `storage show` to list the system-registered storage devices. This ensures that all disks were registered during the disk auto-discovery scan. This also lists the default disk aliases needed for creating your simple volumes.

```
storage show
```

Table 66: Storage Devices

Alias	Entity Name	LUN	Oper. Status	Type
Stor_1	500507606058c90	0	Enabled	disk
Stor_2	2000002037f88fb8	0	Enabled	disk
Stor_3	2000002037c32b1f	0	Enabled	disk
Stor_4	2000002037c32450	0	Enabled	disk

STEP 9. CREATE SIMPLE VOLUMES

Use the CLI command `volume create simple` to create four simple virtual volumes – one from each physical disk.

```
volume create simple -vol Simple1 -d Stor_1
```

```
volume create simple -vol Simple2 -d Stor_2
```

```
volume create simple -vol Simple3 -d Stor_3
```

```
volume create simple -vol Simple4 -d Stor_4
```

STEP 10. CREATE MIRRORED VOLUMES (RAID 1)

Use the CLI command `volume create mirror` to create a mirrored volume, Mirror1, from simple volumes Simple1 and Simple2.

```
volume create mirror -vol Mirror1 -nbc 2 -ch Simple1 -ch Simple2
```

Use the CLI command `volume create mirror` to create a mirrored volume, `Mirror2`, from simple volumes `Simple3` and `Simple4`.

```
volume create mirror -vol Mirror2 -nbc 2 -ch Simple3 -ch Simple4
```

STEP 11. CREATE STRIPED VOLUME (RAID 0)

Use the CLI command `volume create striped` to create a striped volume, `Stripe1`.

```
volume create striped -vol Stripe1 -nbc 2 -sus 64 -ch Mirror1 -ch Mirror2
```

STEP 12. CREATE ISCSI TARGET AND LUN

After creating the final virtual volume configuration that you want to expose to the network host, you need to create an iSCSI target for the volume as well as attach LUN0 to the target volume. Use the CLI command `volume expose -new` to create the iSCSI target and attach LUN0 to the striped volume, `Stripe1`.

```
volume expose -new -vol Stripe1 -ta storage -tn sanrad.billing. -device VSwitch
```

STEP 13. CONFIGURE HOST STATION INITIATOR

Open the Microsoft iSCSI initiator program on host station 1.

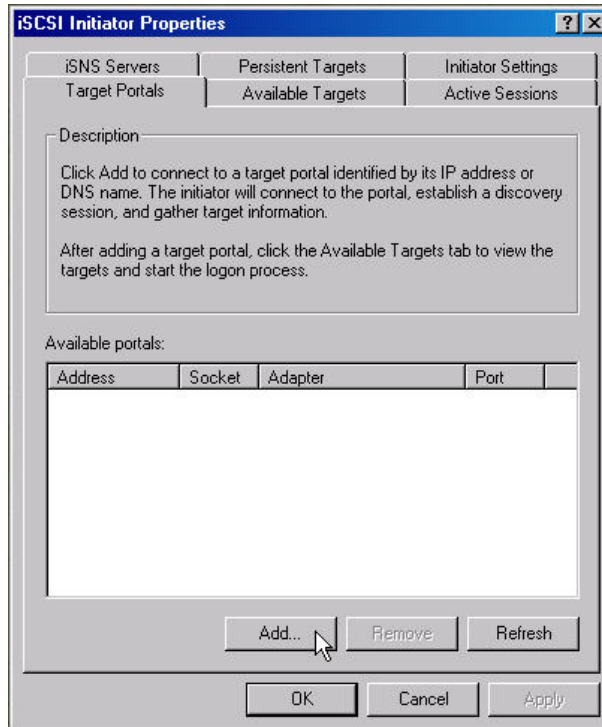


Figure 100. Microsoft iSCSI Initiator

Click **Add** from the **Target Portals** tab. The **Add Target Portal** dialog box opens.

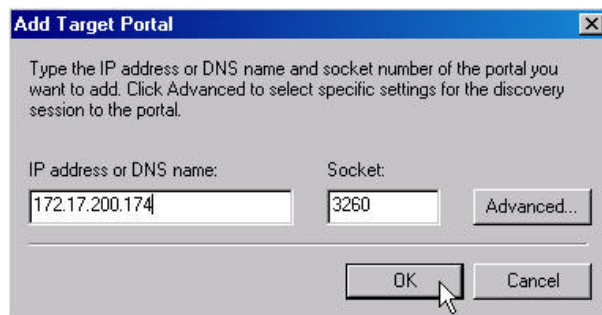


Figure 101. Portal Configuration

Enter the IP address of Eth1, 172.17.200.174 and select the socket for the IP address.

Click **OK**. The Microsoft initiator automatically discovers all available targets for this portal (IP + TCP).

Toggle to the **Available Targets** tab to view all available targets.

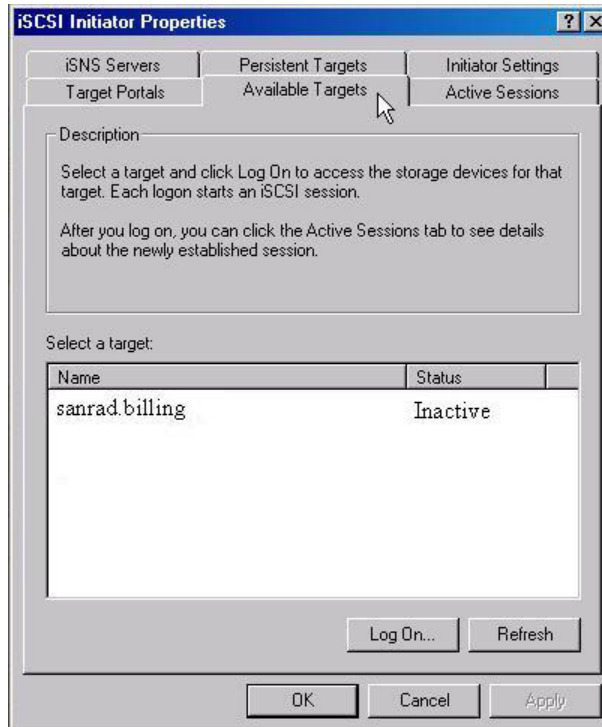


Figure 102. Available Target

STEP 14. BEGIN USING VOLUME

The new disk should be configured as a basic disk only.

You can access Windows' Disk Management application by right clicking on **My Computer** and selecting **Manage**. Select **Disk Management** from the Computer Management window.

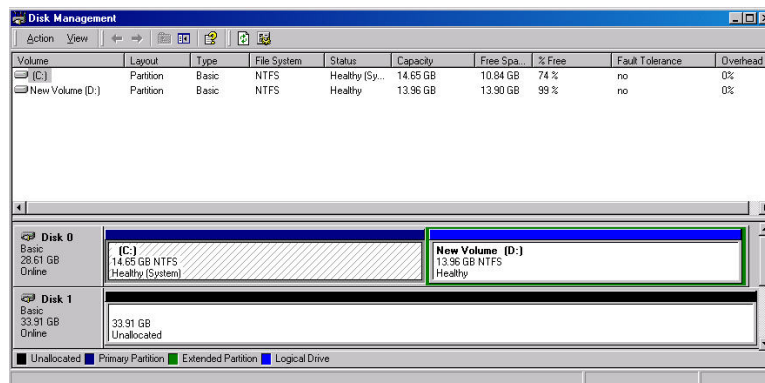


Figure 103. Disk Management Window

Replacing a Mirrored Volume

After configuring the above setup, you notice that Disk 4 in your JBOD has gone offline. Simulate this by removing a physical disk from the JBOD case. You must replace the disk with a new one and reconstruct the volume hierarchy built with the simple volume on Disk 4. Your mirrored volume, Mirror2; created from simple volumes 3 and 4 on disks 3 and 4 respectively, will continue to operate while your physical disk is down and you replace one of its simple volumes.

This example explains how to:

- Identify a failed disk.
- Replace a failed disk.
- Synchronize a volume to an existing mirrored volume.
- Remove a failed volume from the V-Switch database.
- Remove a failed disk from the V-Switch database.

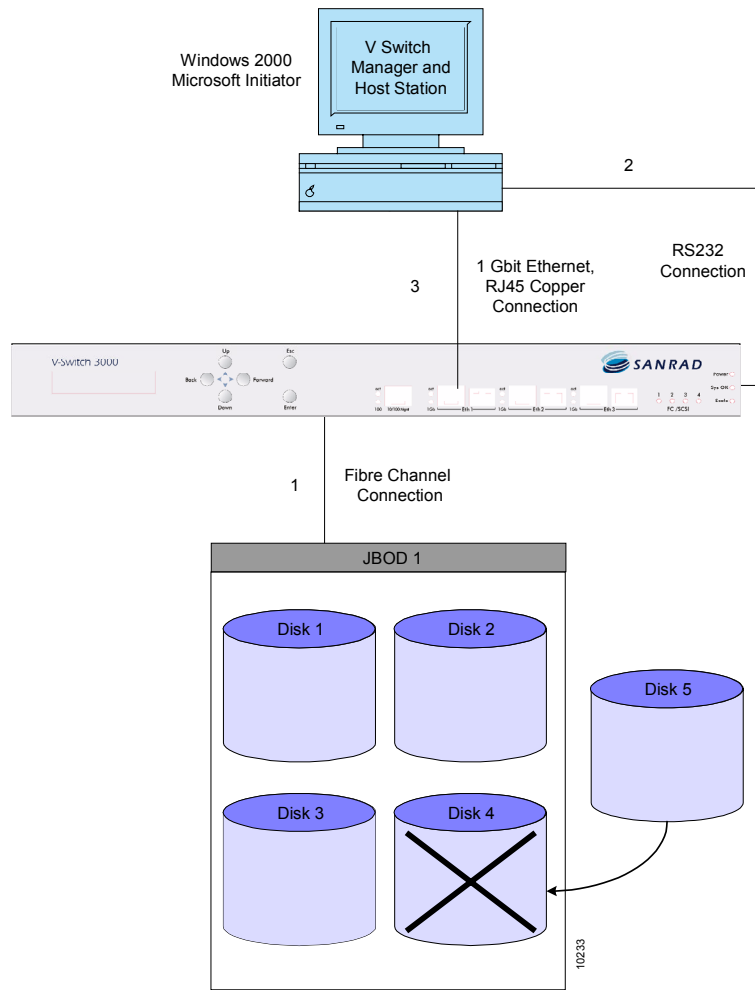


Figure 104. Replacing a Failed Disk

STEP 1. SELECT A REPLACEMENT DISK

Insert a replacement blade of the same size according to your specific manufacture's instructions

STEP 2. CHECK STORAGE DEVICES

Use the CLI command `storage show` to view the new disk's alias. You will need this alias to create a replacement simple volume. Note that the failed disk still appears in the table of storage disks.

Table 67: Storage Devices

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	500507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Storage is missing	entire
Stor_5	500708206059f880	0	Enabled	entire

New disk >

STEP 3. CREATE A SIMPLE VOLUME

Use the CLI command `volume create simple` to create a simple volume from the newly inserted disk.

```
volume create simple -vol Simple5 -d Stor_5
```

STEP 4. REPLACE FAILED VOLUME

Use the CLI command `volume replace` to replace simple volume 4 which sat on the failed disk with simple volume 5 in the mirrored volume hierarchy.

```
volume replace -vol Simple4 -nvol Simple5
```

STEP 5. CHECK VOLUME STATUS

Use the CLI command `volume show` to view the volume status. Note that Simple4 is defined as Nonfunctional while Simple5 is defined as NeedSync.

Alias	Vol Type	# of Blocks	Block Size	State
Simple3	Simple	1024	512	Exposed
Simple4	Simple	1024	512	Nonfunct
Simple5	Simple	1024	512	NeedSync
Mirror2	Mirror	1024	512	Exposed

STEP 6. SYNCHRONIZE MIRROR

Use the CLI command `volume mirror synch` to synchronize the new volume data with its intact mirrored volume, Simple3. Once you execute this command, the new mirrored volume will be fully functional.

```
volume mirror synch -src Simple3 -dst Simple5
```

The synchronization is finished when the volume status of Simple5 changes from NeedSync to Exposed.

STEP 7. REMOVE FAILED VOLUME

Use the CLI command `volume remove all` to remove the non-functional virtual volume from the V-Switch database.

```
volume remove all -vol Simple4
```

STEP 8. REMOVE FAILED DISK

Use the CLI command `storage remove` to remove the failed disk from the V-Switch database.

```
storage remove -s Stor_4
```

Use the CLI command `storage show` to view the updated storage disk table.

Table 68: Failed Storage Disk Removed

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	500507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_5	500708206059f880	0	Enabled	entire

Replicating Data Off-line

You have a four-disk legacy JBOD. You want to upgrade to a new JBOD and need to replicate the contained data from the old device to the new device as expediently as possible. None of the disks are virtualized or exposed. You must virtualize all of the physical disks to simple volumes with the same capacity and block size. If the new disks are larger than the old disks, you must first create subdisks of the same capacity as the old disks before creating simple volumes. Then replicate the data from the old volumes to the new volumes. When the replication is complete, you are left with two independent data copies from each original volume.

This example explains how to:

- Create simple volumes.
- Replicate data from one child of a mirror to the other child.

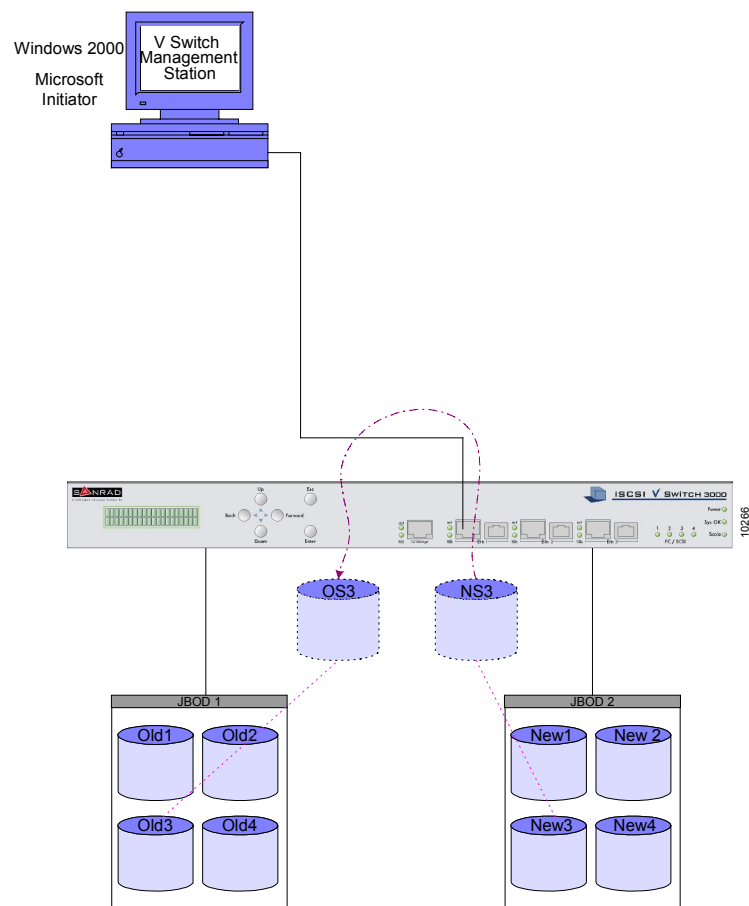


Figure 105. Replicating Data Off-line

STEP 1. ATTACH AND VIEW STORAGE DEVICES

Attach the legacy JBOD to the V-Switch and configure the storage port communications as needed. See "Configuring the Storage Ports," page 57.

Use the CLI command `storage show` to view the attached storage.

Table 69: Legacy JBOD Disks

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	200507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire

Next, attach the new JBOD to the V-Switch and configure the storage port communications as needed.

Use the CLI command `storage show` to view the attached storage. The legacy JBOD disks are Stor_1 through Stor_4. The new JBOD disks are Stor_5 through Stor_8.

Table 70: Legacy + New JBOD Disks

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	200507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire
Stor_5	500708206059f880	0	Enabled	entire
Stor_6	500003504206a683	0	Enabled	entire
Stor_7	500065470490f321	0	Enabled	entire
Stor_8	500000024364h764	0	Enabled	entire

STEP 2. CREATE SIMPLE VOLUMES

Use the CLI command `volume create simple` to create a simple volume from each disk.

Use one standard for naming the legacy JBOD simple volumes and another for naming the new JBOD simple volumes. This will provide a visual cue when it is time to designate the source volume to replicate from.

```
volume create simple -vol OS1 -d Stor_1
volume create simple -vol OS2 -d Stor_2
. . .
volume create simple -vol NS3 -d Stor_7
volume create simple -vol NS4 -d Stor_8
```

STEP 3. REPLICATE DATA

Use the CLI command `volume copy create` to begin replicating the data. The legacy volume is the source volume. The new volume is the destination volume.

```
volume copy create -src OS1 -dst NS1
```

```
volume copy create -src OS2 -dst NS2
```

```
volume copy create -src OS3 -dst NS3
```

```
volume copy create -src OS4 -dst NS4
```

STEP 4. CHECK REPLICATION STATUS

Use the CLI command `volume mirror show` to check the replication status.

Table 71: Replication Status

Source	Destination	Oper Status	Admin Status	Progress
NONE	OS1	synch	None	0
OS1	NS1	synch	dataRep	25
NONE	OS2	synch	None	0
OS2	NS2	synch	dataRep	13
NONE	OS3	synch	None	0
OS3	NS3	synch	dataRep	7
NONE	OS4	synch	None	0
OS4	NS4	synch	dataRep	2

The simple volumes can be exposed independently to hosts or used as building blocks in another volume hierarchy.

Configuring the V-Switch with a Single IP Routing Path

You have just purchased a V-Switch to manage your company's storage network. A section of your company's employees is located in your local branch offices and a section is stationed in your overseas offices.

You need to configure volume access for both the local and overseas employees.

In this example, the storage network consists of:

- One JBOD appliance with four disks of equal capacity (the actual capacity is not important) connected to the V-Switch.
- One computer terminal with a network card (NIC) acting as the management station for the V-Switch connected to the Ethernet port Eth1 via a 1 Gbit Ethernet RJ45 cable. See #2 in Figure 106, page 264.
- One LAN connection to Ethernet port Eth2 via a 1 Gbit Ethernet RJ45 cable. See #3 in Figure 106, page 264.
- One external network connection to the LAN.

The hosts 1 and 2 run on the Windows™ 2000 platform and have the IBM iSCSI initiator v.1.2.2 software installed.

An IP address has already been assigned to the management station.

The management port Eth 1 IP address will be assigned 100.100.100.2.

The network port Eth 2 IP address will be assigned 212.199.43.56.

The iSCSI portal for network port Eth2 will be set to 5003.

Your network should mimic Figure 106, page 264.

This example explains how to:

- Initialize your V-Switch via the LCD display panel and control buttons.
- Manage your V-Switch through a direct 1 Gbit Ethernet connection to the V-Switch Eth 1 network port.
- Configure IP routing to a remote IP network.
- Configure network port Eth 2 for volume exposure to hosts.
- Create a RAID 10 volume.
- Expose a RAID 10 volume to both local and remote hosts.

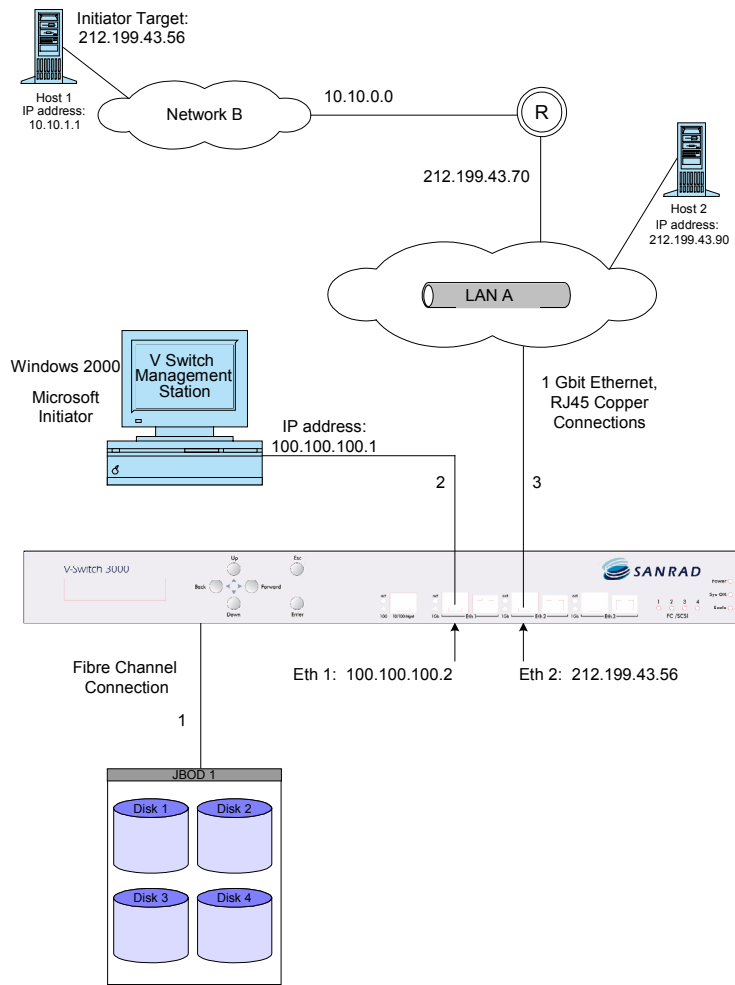


Figure 106. IP Routing Topology

STEP 1. ATTACH CABLES

Attach an HSSDC-DB9 fibre channel cable from your JBOD appliance to one of the storage ports on the back panel of the V-Switch. See #1 in Figure 106, page 264. Depending on your appliance, you need to plug a terminator into one of the JBOD ports.

Attach an RJ45 copper 1 Gbit Ethernet cable from the Ethernet port **Eth1** on the front panel of the V-Switch to your management station.

STEP 2. POWER UP STORAGE DEVICE

Power up the JBOD appliance first to allow the V-Switch to register it in its network scan.

STEP 3. POWER UP V-SWITCH

Connect the power cord to the V-Switch and then to the electric socket. The V-Switch powers up. The fan assembly is running and the LCD panel displays:

```
V-Switch 3000
Status: OK
```

STEP 4. INITIALIZE V-SWITCH

Use the LCD display and control buttons to configure the V-Switch management port IP address and mask.

Use the LCD display and control buttons on the V-Switch to configure the V-Switch management port IP address and mask.

- Toggle to the IP Configure ETH1 Port screen.
- Press **Enter**. The **IP Configuration** screen appears.

```
IP CONFIG
```

- Press Enter again. The IP Config ETH1 Port screen appears.

```
IP Config
ETH1 Port
```

- Press Enter. The Insert IP screen appears.

```
Insert IP
0 0 0.0 0 0.0 0 0.0 0 0
```

- Enter the management port IP address. The left/right buttons toggle between places in the IP address. The up/down buttons scroll between numbers. Press Enter after inputting the full address.

```
Insert IP
1 0 0.1 0 0.1 0 0.0 0 2
```

- Press Enter to enter the IP address and progress to the IP Mask screen.

```
Mask
2 5 5.2 5 5.2 5 5.0 0 0
```

- If you want to change from the default mask, use the left/right buttons to toggle between places in the mask and the up/down buttons scroll between numbers.

- Press Enter to enter the IP mask and return to the main V-Switch Status screen.

```
V-Switch 3000
Status: OK
```

STEP 5. LOGIN TO THE MANAGEMENT PORT

From your management terminal, open a Telnet session with the management port.

- From the Windows Start menu, select Run.
- In the Open window, enter:
`telnet 100.100.100.2`
- Click OK. A Telnet session window opens.
- Press Enter on your keyboard to open the V-Switch 3000 Login window.



Figure 107. V-Switch 3000 Login Screen

- Enter the default user name and password and press Enter on your keyboard. The CLI prompt `>` appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

STEP 6. CONFIGURE NETWORK PORT ETH 2 IP ADDRESS

Use the CLI command `ip config set` to configure the network port Eth 2 for communications between the V-Switch and host stations.

```
ip config set -if eth2 -ip 212.199.43.56 -im
255.255.255.0 -act 1
```

STEP 7. CONFIGURE iSCSI PORTAL

Use the CLI command `iscsi portal create` to configure the iSCSI portal on network port Eth 1 for iSCSI communications between the V-Switch and the host station.

```
iscsi portal create -ip 212.199.43.56 -p 5003
```

The port number you set in the CLI must coincide with the port number you set in your iSCSI initiator configuration.

STEP 8. CONFIGURE IP ROUTING PATH

Use the CLI command `ip route add` to create an IP routing path to the external host network IP address from network port Eth 2. This will allow communications between the local V-Switch and Network B's host stations.

```
ip route add -dip 10.10.0.0 -dmask 255.255.255.0 -gw 212.199.43.70 -if eth2
```

STEP 9. CHECK STORAGE DEVICES

Use the CLI command `storage show` to list the system-registered storage devices. This ensures that all disks were registered during the disk auto-discovery scan. This also lists the default disk aliases needed for creating your virtual volumes.

```
storage show
```

Table 72: Storage Disks

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	500507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire

STEP 10. CREATE SIMPLE VOLUMES

Use the CLI command `volume create simple` to create four simple virtual volumes – one from each physical disk.

```
volume create simple -vol Simple1 -d Stor_1
```

```
volume create simple -vol Simple2 -d Stor_2
```

```
volume create simple -vol Simple3 -d Stor_3
```

```
volume create simple -vol Simple4 -d Stor_4
```

STEP 11. CREATE MIRRORED VOLUMES (RAID 0)

Use the CLI command `volume create mirror` to create a mirrored volume, Mirror1, from simple volumes Simple1 and Simple2.

```
volume create mirror -vol Mirror1 -nbc 2 -ch Simple1 -ch Simple2
```

Use the CLI command `volume create mirror` to create a mirrored volume, Mirror2, from simple volumes Simple3 and Simple4.

```
volume create mirror -vol Mirror2 -nbc 2 -ch Simple3 -ch Simple4
```

STEP 12. CREATE STRIPED VOLUME (RAID 1)

Use the CLI command `volume create striped` to create a striped volume, Stripe1.

```
volume create striped -vol Stripe1 -nbc 2 -sus 64 -ch Mirror1 -ch Mirror2
```

STEP 13. CREATE ISCSI TARGET AND LUN

After creating the final virtual volume configuration that you want to expose to the network hosts, you need to create an iSCSI target for the volume as well as attach LUN0 to the target volume. Use the CLI command `volume expose -new` to create the iSCSI target and attach LUN0 to the striped volume, Stripe1.

```
volume expose -new -vol Stripe1 -ta storage -tn billing.sanrad -device VSwitch
```

STEP 14. CONFIGURE HOST STATION INITIATOR

Open the Microsoft iSCSI initiator program on host station 1.

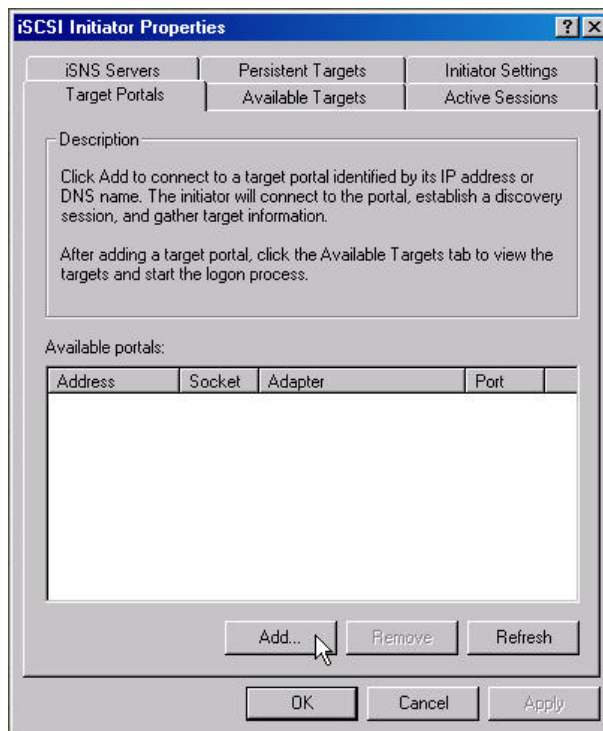


Figure 108. Microsoft iSCSI Initiator

Click **Add** from the **Target Portals** tab. The **Add Target Portal** dialog box opens.

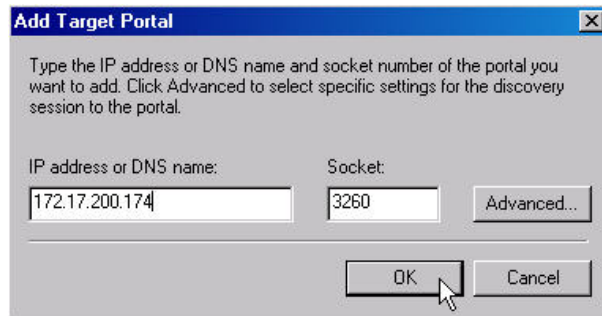


Figure 109. Portal Configuration

Enter the IP address of Eth1, 172.17.200.174 and select the socket for the IP address.

Click **OK**. The Microsoft initiator automatically discovers all available targets for this portal (IP + TCP).

Toggle to the **Available Targets** tab to view all available targets.

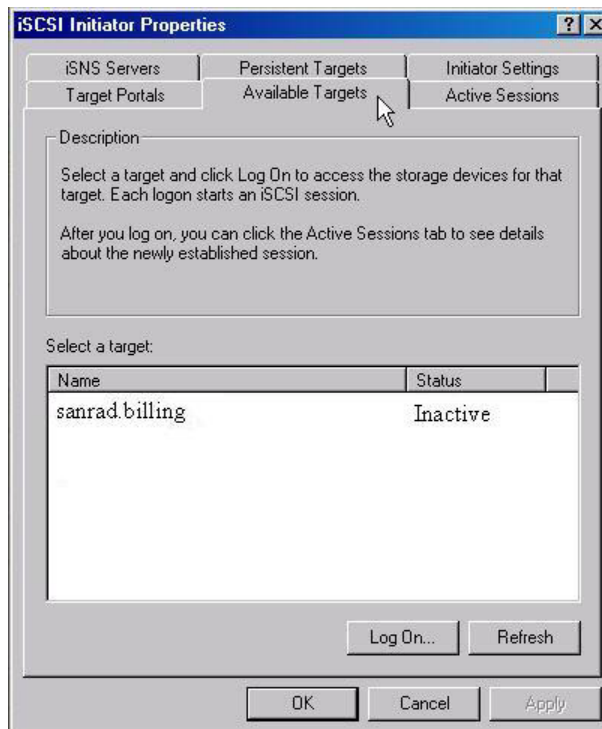


Figure 110. Available Target

STEP 15. BEGIN USING VOLUME

The new disk should be configured as a basic disk only.

You can access Windows' Disk Management application by right clicking on **My Computer** and selecting **Manage**. Select **Disk Management** from the Computer Management window.

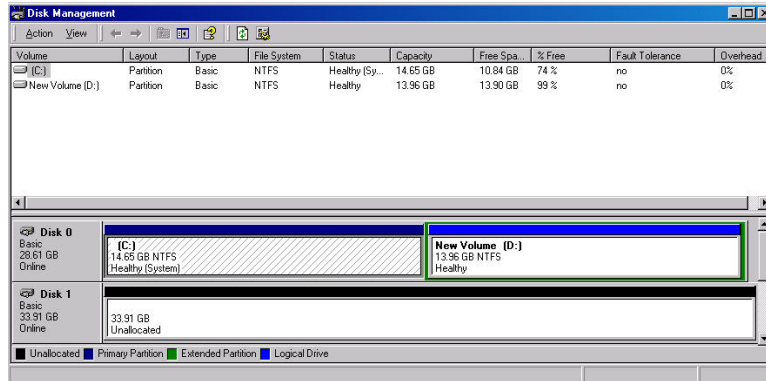


Figure 111. Disk Management Window

Configuring a Cluster

You have just purchased two V-Switches and are ready to configure your host/storage network. Your company has one LAN for storage access and V-Switch management connections.

Your management station IP address is 212.199.43.40.

You have one FC JBOD that contains four disks.

Because you have only one company LAN, you will be using only one network port, Eth 2, to connect the V-Switches to the company hosts. Your LAN mask is 212.199.43.

You have two hosts 1 and 2 with Microsoft iSCSI initiators and running on Windows™ 2000 OS.

You will create identical V-Switch and volume configuration files for each V-Switch, with only the V-Switch aliases being unique.

You will create two mirrored volumes, Mirror1 and Mirror2, one to be exposed on V-Switch 1 to one host and one to be exposed on V-Switch 2 to both hosts.

This example explains how to:

- Initialize the V-Switches via the LCD display panel and control buttons.
- Name the V-Switches.
- Identify a physical disk on multiple V-Switches.
- Manage the V-Switches via terminal and Telnet session.
- Configure a network port for IP takeover in the event that a neighboring V-Switch goes offline.
- Configure a cluster.
- Enable host access to more than one iSCSI target.

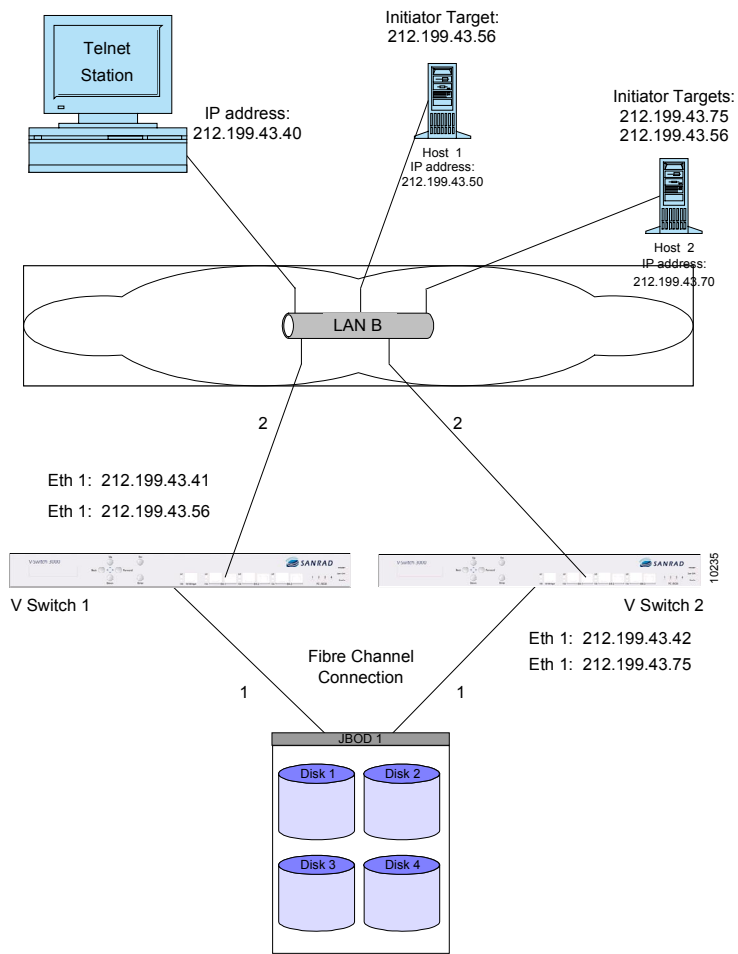


Figure 112. Cluster Topology

STEP 1. ATTACH CABLES

Attach an HSSDC-DB9 fibre channel cable from your JBOD appliance to one of the storage ports on the back panel of V-Switch 1. See #1 in Figure 112. Depending on your appliance, you need to plug a terminator into one of the JBOD ports.

Attach an RJ45 copper 1 Gbit Ethernet cable from the Ethernet port **Eth1** on the front panel of V-Switch 1 to your Telnet terminal. See #2 in Figure 112. Attach another RJ45 copper 1 Gbit Ethernet cable from the Ethernet port **Eth1** on the front panel of the second V-Switch, Vswitch2, to your Telnet terminal.

STEP 2. POWER UP STORAGE DEVICE

Power up the JBOD appliance first to allow both V-Switches to register it in their network scan.

STEP 3. POWER UP V-SWITCHES

Connect the power cord to V-Switch 1 and then to the electric socket. The V-Switch powers up. The fan assembly is running and the LCD panel displays:

```
V-Switch 3000
Status: OK
```

Connect the power cord to V-Switch 2 and then to the electric socket. The V-Switch powers up. The fan assembly is running and the LCD panel displays:

```
V-Switch 3000
Status: OK
```

STEP 4. INITIALIZE V-SWITCH 1

Use the LCD display and control buttons on V-Switch 1 to configure the V-Switch management port IP address and mask.

- Toggle to the IP Configure ETH1 Port screen.
- Press **Enter**. The **IP Configuration** screen appears.

```
IP CONFIG
```

- Press **Enter** again. The **IP Config ETH1 Port** screen appears.

```
IP Config
ETH1 Port
```

- Press Enter. The Insert IP screen appears.

```
Insert IP
0 0 0.0 0 0.0 0 0.0 0 0
```

- Enter the management port IP address. The left/right buttons toggle between places in the IP address. The up/down buttons scroll between numbers. Press Enter after inputting the full address.

```
Insert IP
2 1 2.1 9 9.0 4 3.0 4 1
```

- Press Enter to enter the IP address and progress to the IP Mask screen.

```
Mask
2 5 5.2 5 5.2 5 5.0 0 0
```

- If you want to change from the default mask, use the left/right buttons to toggle between places in the mask and the up/down buttons scroll between numbers.
- Press Enter to enter the IP mask and return to the main V-Switch Status screen.

```
V-Switch 3000
Status: OK
```


STEP 5. INITIALIZE V-SWITCH 2

Use the LCD display and control buttons on V-Switch 2 to configure the V-Switch management port IP address and mask.

- Toggle to the IP Configure ETH1 Port screen.
- Press **Enter**. The **IP Configuration** screen appears.

```
IP CONFIG
```
- Press **Enter** again. The **IP Config ETH1 Port** screen appears.

```
IP Config
ETH1 Port
```
- Press Enter. The Insert IP screen appears.

```
Insert IP
0 0 0.0 0 0.0 0 0.0 0 0
```
- Enter the management port IP address. The left/right buttons toggle between places in the IP address. The up/down buttons scroll between numbers. Press Enter after inputting the full address.

```
Insert IP
2 1 2.1 9 9.0 4 3.0 4 2
```
- Press Enter to enter the IP address and progress to the IP Mask screen.

```
Mask
2 5 5.2 5 5.2 5 5.0 0 0
```
- If you want to change from the default mask, use the left/right buttons to toggle between places in the mask and the up/down buttons scroll between numbers.
- Press Enter to enter the IP mask and return to the main V-Switch Status screen.

```
V-Switch 3000
Status: OK
```

STEP 6. LOGIN TO THE V-SWITCH 1 MANAGEMENT PORT

From your management terminal, open a Telnet session with the management port on V-Switch 1.

- From the Windows Start menu, select Run.
- In the Open window, enter:

```
telnet 212.199.43.41
```
- Click OK. A Telnet session window opens.
- Press Enter on your keyboard to open the V-Switch 3000 Login window.



Figure 113. V-Switch 3000 Login Screen

- Enter the default user name, **sanrad**, and password, **sanrad**, and press **Enter** on your keyboard. The CLI prompt **>** appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

STEP 7. NAME V-SWITCH 1

Use the CLI command `init` to name V-Switch 1. You will need this name later for exposing volumes.

```
init -n VSwitch1
```

STEP 8. LOGIN TO THE V-SWITCH 2 MANAGEMENT PORT

From your management terminal, open another Telnet session, this time with the management port on V-Switch 2.

- From the Windows Start menu, select Run.
- In the Open window, enter:
`telnet 212.199.43.42`
- Click OK. A Telnet session window opens.
- Press Enter on your keyboard to open the V-Switch 3000 Login window.



Figure 114. V-Switch 3000 Login Screen

- Enter the default user name and password and press **Enter** on your keyboard. The CLI prompt **>** appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

keyboard. The CLI prompt `>` appears. You are now logged in and ready to begin configuring your V-Switch for volume virtualization and exposure.

STEP 9. NAME V-SWITCH 2

Use the CLI command `init` to name V-Switch 2. You will need this name later for exposing volumes.

```
init -n VSwitch2
```

STEP 10. CREATE CLUSTER

You need to enable your two V-Switches to act as one unit to provide V-Switch failover. To do this, you need to tell each one that the other one exists. Use the CLI command `neighbor add` to tell each V-Switch that it has a neighbor.

To V-Switch 1, add V-Switch 2 as a neighbor.

```
neighbor add -nb VSwitch2 -ip 212.199.43.42
```

To V-Switch 2, add V-Switch 1 as a neighbor.

```
neighbor add -nb VSwitch1 -ip 212.199.43.41
```

STEP 11. CONFIGURE V-SWITCH 1 NETWORK PORT ETH 1 IP ADDRESSES

Use the CLI command `ip config set` to configure the network port Eth 1 for communications between VSwitch1 and the host stations on VSwitch1. Set the IP address as active (1) to allow read/write commands to pass through this IP address.

```
ip config set -if eth1 -ip 212.199.43.56 -im  
255.255.255.0 -act 1
```

Now, use the CLI command `ip config set` to configure the IP takeover address for Eth 1. This IP address will be the IP address of Eth 1 on VSwitch2. The address will sit inactive (2) unless VSwitch2 goes offline. Then VSwitch1 will activate (1) this address and direct all read/write commands to this address through Eth1 on VSwitch1.

```
ip config set -if eth1 -ip 212.199.43.75 -im  
255.255.255.0 -act 2
```

STEP 12. CONFIGURE V-SWITCH 1 iSCSI PORTALS

Use the CLI command `iscsi portal create` to configure the iSCSI portal on network port Eth 2 for iSCSI communications between VSwitch1 and the host stations.

```
iscsi portal create -ip 212.199.43.56 -p 5003
```

The port number you set in the CLI must coincide with the port number you set in your iSCSI initiator configuration.

Use the CLI command again to configure the iSCSI portal for the inactive IP address on Eth 2 to allow iSCSI communications via this IP on VSwitch1 in the event of VSwitch2 failover.

```
iscsi portal create -ip 212.199.43.75 -p 5003
```

STEP 13. CONFIGURE V-SWITCH 2 NETWORK PORT ETH 1 IP ADDRESSES

Use the CLI command `ip config set` to configure the network port Eth 1 for communications between VSwitch2 and the host stations on VSwitch2. Set the IP address as active (1) to allow read/write commands to pass through this IP address.

```
ip config set -if eth1 -ip 212.199.43.75 -im  
255.255.255.0 -act 1
```

Now, use the CLI command `ip config set` to configure the IP takeover address for Eth 1. This IP address will be the IP address of Eth 1 on VSwitch1. The address will sit inactive (2) unless V-Switch 1 goes offline. Then VSwitch2 will activate (1) this address and direct all read/write commands to this address through Eth 1 on VSwitch2.

```
ip config set -if eth1 -ip 212.199.43.56 -im  
255.255.255.0 -act 2
```

STEP 14. CONFIGURE V-SWITCH 2 ISCSI PORTALS

The port number you set in the CLI must coincide with the port number you set in your iSCSI initiator configuration.

Use the CLI command `iscsi portal create` to configure the iSCSI portal on network port Eth 1 for iSCSI communications between the V-Switch and the host stations.

```
iscsi portal create -ip 212.199.43.75 -p 5003
```

Use the CLI command again to configure the iSCSI portal for the inactive IP address on Eth 1 to allow iSCSI communications via this IP on VSwitch2 in the event of VSwitch1 failover.

```
iscsi portal create -ip 212.199.43.56 -p 5003
```

STEP 15. CHECK STORAGE DEVICES

Use the CLI command `storage show` to list the system-registered storage devices on VSwitch1. This ensures that all disks were registered during the disk auto-discovery scan. This also lists the default disk aliases needed for creating your simple volumes.

```
storage show
```

Table 73: Storage Disks as seen through V-Switch 1

Use the unique disk entity names (WWUIs) and NOT the default disk aliases to duplicate virtual volume hierarchies in each V-Switch.

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	2000002037f88fb8	0	Enabled	entire
Stor_2	500507606058c90	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire

Use the CLI command `storage show` to list the system-registered storage devices on VSwitch2. This ensures that all disks were registered during the disk auto-discovery scan. This also lists the default disk aliases needed for creating your simple volumes.

```
storage show
```

Table 74: Storage Disks as seen through V-Switch 2

Use the unique disk entity names (WWUIs) and NOT the default disk aliases to duplicate virtual volume hierarchies in each V-Switch.

Alias	Entity Name	LUN	Oper. Status	Subdisk
Stor_1	500507606058c90	0	Enabled	entire
Stor_2	2000002037f88fb8	0	Enabled	entire
Stor_3	2000002037c32b1f	0	Enabled	entire
Stor_4	2000002037c32450	0	Enabled	entire

Compare this disk table with the disk table from VSwitch1. Note that Default storage 1 and 2 are reversed in the disk table from VSwitch2. That is, Default storage 1 in VSwitch1 is listed as Default storage 2 in VSwitch2. You will use the WWUIs to duplicate virtual volume hierarchies in each V-Switch.

STEP 16. CREATE SIMPLE VOLUMES ON V-SWITCH 1

Use the CLI command `volume create simple` to create four simple virtual volumes – one from each physical disk.

```
volume create simple -vol Simple1 -d Stor_1
```

```
volume create simple -vol Simple2 -d Stor_2
```

```
volume create simple -vol Simple3 -d Stor_3
```

```
volume create simple -vol Simple4 -d Stor_4
```

STEP 17. CREATE MIRRORED VOLUMES (RAID 0)

Use the CLI command `volume create mirror` to create a mirrored volume, Mirror1, from simple volumes Simple1 and Simple2.

```
volume create mirror -vol Mirror1 -nbc 2 -ch Simple1 -ch Simple2
```

Use the CLI command `volume create mirror` to create a mirrored volume, `Mirror2`, from simple volumes `Simple3` and `Simple4`.

```
volume create mirror -vol Mirror2 -nbc 2 -ch Simple3 -ch Simple4
```

STEP 18. CREATE ISCSI TARGET AND LUN

After creating the final virtual volume that you want to expose to the network host, you need to create an iSCSI target for the volumes as well as attach LUN0 to each target volume. Use the CLI command `volume expose -new` to create each iSCSI target and attach LUN0 to each mirrored volume, `Mirror1` and `Mirror2`.

```
volume expose -new -vol Mirror1 -ta billing -tn billing.sanrad -device VSwitch1
```

```
volume expose -new -vol Mirror2 -ta musicbox -tn musicbox.sanrad -device VSwitch2
```

STEP 19. CREATE SIMPLE VOLUMES ON V-SWITCH 2

Now you will repeat the volume configurations on `VSwitch2` to mimic the configurations on `VSwitch1`. Use the CLI command `volume create simple` to create four simple virtual volumes – one from each physical disk. Note that, using the WWUI to identify each disk, `Simple1` is built on default storage 2 and `Simple 2` is built on default storage 1.

```
volume create simple -vol Simple1 -d Stor_2
```

```
volume create simple -vol Simple2 -d Stor_1
```

```
volume create simple -vol Simple3 -d Stor_3
```

```
volume create simple -vol Simple4 -d Stor_4
```

STEP 20. CREATE MIRRORED VOLUMES (RAID 0)

Use the CLI command `volume create mirror` to create a mirrored volume, `Mirror1`, from simple volumes `Simple1` and `Simple2`.

```
volume create mirror -vol Mirror1 -nbc 2 -ch Simple1 -ch Simple2
```

Use the CLI command `volume create mirror` to create a mirrored volume, `Mirror2`, from simple volumes `Simple3` and `Simple4`.

```
volume create mirror -vol Mirror2 -nbc 2 -ch Simple3 -ch Simple4
```

STEP 21. CREATE ISCSI TARGET AND LUN

After creating the final virtual volume that you want to expose to the network host, you need to create an iSCSI target for the volumes as well as attach LUN0 to each target volume. Use the CLI command `volume expose -new` to create each iSCSI target and attach LUN0 to each mirrored volume, Mirror1 and Mirror2.

```
volume expose -new -vol Mirror1 -ta billing -tn sanrad.  
billing -device VSwitch1
```

```
volume expose -new -vol Mirror2 -ta musicbox -tn sanrad.  
musicbox -device VSwitch2
```

STEP 22. CONFIGURE HOST STATION 1 INITIATOR

Open the Microsoft iSCSI initiator program on host station 1.

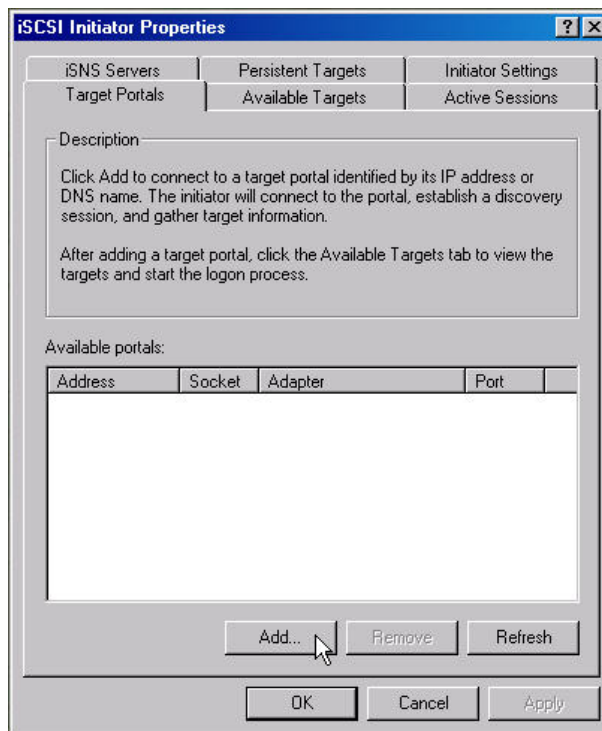


Figure 115. Microsoft iSCSI Initiator

Click **Add** from the **Target Portals** tab. The **Add Target Portal** dialog box opens.

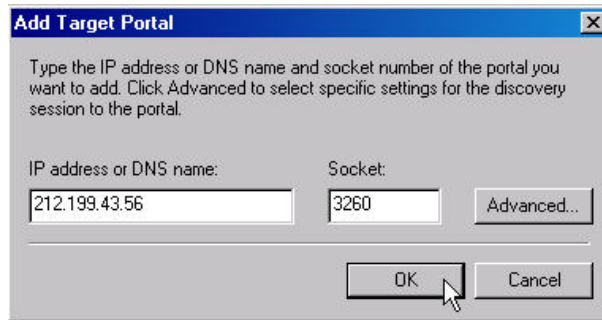


Figure 116. Portal Configuration

Enter the IP address of Eth1, 212.199.43.56 and select the socket for the IP address.

Click **OK**. The Microsoft initiator automatically discovers all available targets for this portal (IP + TCP).

Toggle to the **Available Targets** tab to view all available targets for the configured portal.

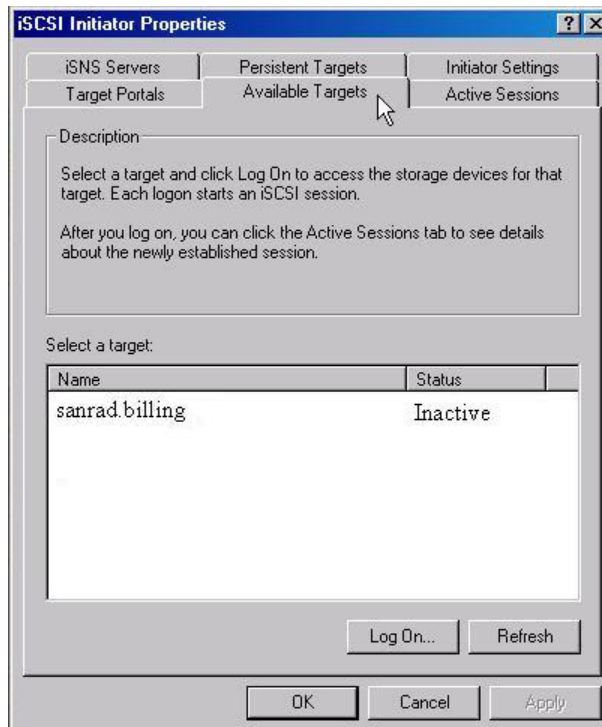


Figure 117. Available Target

STEP 23. CONFIGURE HOST STATION 2 INITIATOR

Open the Microsoft iSCSI initiator program on host station 2.

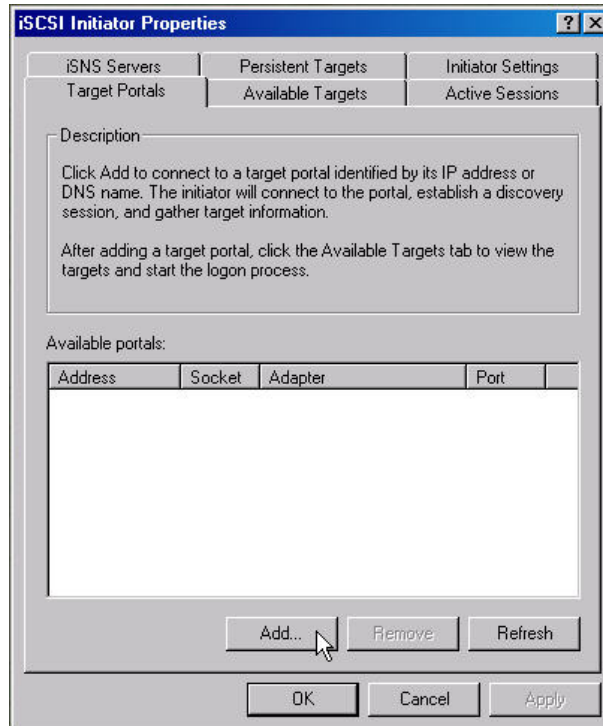


Figure 118. Microsoft iSCSI Initiator

Click **Add** from the **Target Portals** tab. The **Add Target Portal** dialog box opens.

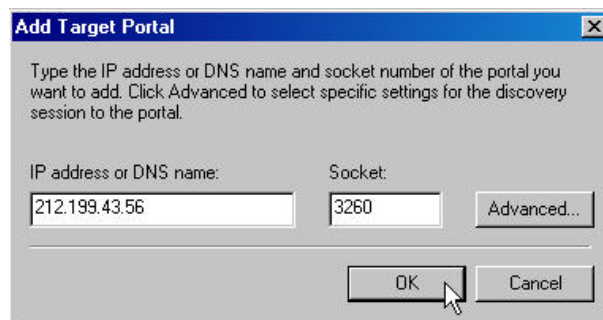


Figure 119. Portal Configuration

Enter the IP address of Eth1, 212.199.43.56 and select the socket for the IP address.

Click **OK**. The Microsoft initiator automatically discovers all available targets for this portal (IP + TCP).

Toggle to the **Available Targets** tab to view all available targets for the configured portal.

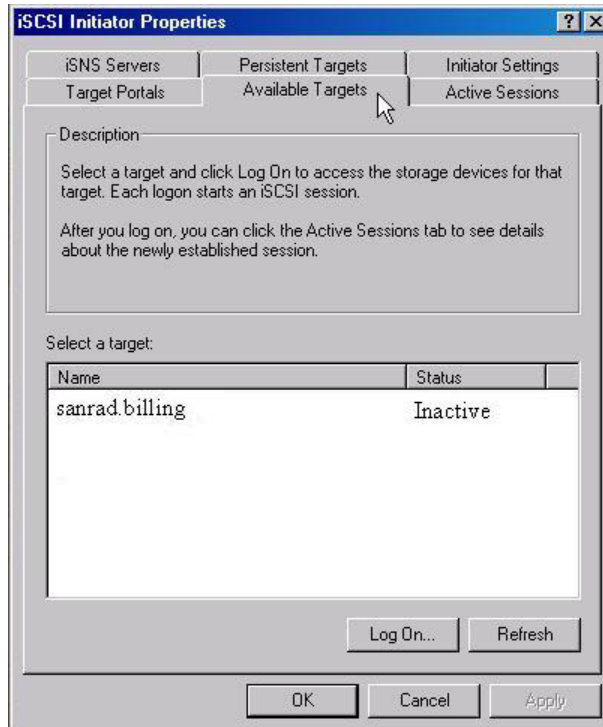


Figure 120. Available Target

Because host 2 has access to two targets, you need to add the second initiator to access the target, sanrad.musicbox.

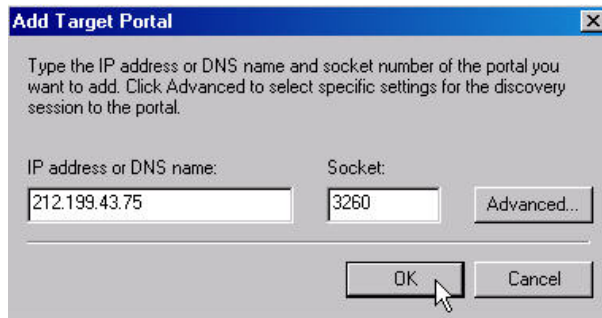


Figure 121. 2nd Microsoft iSCSI Initiator Configuration for Host Station 2

Toggle to the **Available Targets** tab to view all available targets for the host 2 initiator.

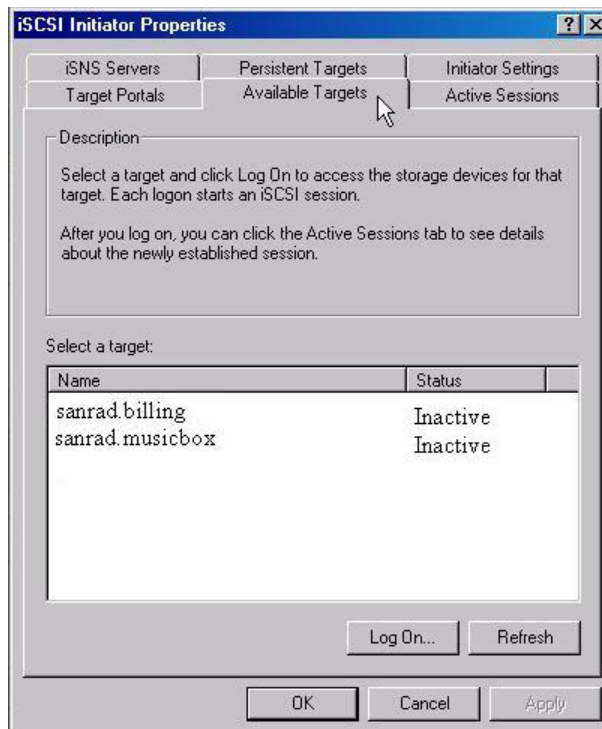


Figure 122. All Available Targets



I

1

10/10019

A

AC power supplies 186

ACL

add236
details236
down241
identity add chap239
identity add name239
identity add srp240
identity create238
identity delete238
identity details..... 128, 238
identity remove chap240
identity remove name.....239
identity remove srp240
identity set.....241
remove237
set237
show 117, 235, 237
up241

Actual capacity 153, 158

Add

acl236
acl identity chap239

Index

acl identity srp240
admin 55, 199
IP route67, 180, 207
iSNS 63, 174
mirror229
neighbor 76, 209
RADIUS 129, 242
SNMP manager 54, 204
user profile175

Add name

acl identity239

Admin

add 175, 199
password 175, 199
remove 175, 199
show198

Alias

disk217
iSCSI target234
storage217
subdisk 90, 221
volume93, 162, 223

Auto-discovery 28, 38

B

Blink

storage abort..... 86, 216
storage activate 85, 216

Boot213

Break	
mirror.....	150, 229
Bridging switch	16
Bus ID	57, 204

C

Capacity	
actual.....	153, 158
potential	153, 158
Change	
password	175
user profile.....	175
CHAP	
add acl identity	239
remove identity	240
Chassis	22, 34
Check	
IP route	68
CLI.....	19, 195
Cluster.....	72
configuration	69, 79, 271
failover disable	79, 185, 211
failover enable.....	79, 185, 211
set	82, 185, 211
show	78, 210
Command Line Interface	19
Community	55
Compact Flash Slot.....	42
Concatenated	
volume	224
Configure	
cluster	69, 79, 271
console.....	49, 177
IP routing.....	66
IP set	251
iSCSI.....	64, 108
network ports	60
storage port	57
V-Switch cluster.....	75
V-Switch single IP	263
V-Switch via console	49, 177
V-Switch via LCD	48
Console.....	249
config	49, 177
Console port.....	30, 40
Corrupted database.....	191

Create	
acl identity	238
concatenated volume.....	95, 224
iSCSI portal.....	64, 233
iSCSI target	234
mirrored volume	224
RAID 0+1.....	106
simple volume	93, 223
snapshot	146
stripe volume	97, 225
subdisk	90, 219
transparent volume	224
volume copy	262
volume mirror.....	100
volume RAID 0+1	103
volume RAID 10.....	103
volume simple	93
Cube	153

D

Data replication .	102, 140, 260, 262
Database	
corrupted	192, 213
download	177, 212
export.....	192, 213
upload	176, 212
Dead interval.....	78, 211
Default	
gateway	67
Default factory database	191
Default factory system.....	191
Delete	
acl identity	238
iSNS.....	64, 168, 174
RADIUS	168
Details	
acl.....	236
disk	87, 218
interface	203
iSCSI target	117
LU	245
LUN	245
neighbor	80, 210
storage	87, 218
subdisk	91
subdisks.....	220

- volume222
- Device
 - set46, 52, 75, 170, 182, 200
 - set Telnet..... 54, 171, 201
- Disable
 - cluster failover..... 79, 185, 211
- Discover
 - storage216
- Discover LUNs 181, 201
- Disk
 - alias217
 - details 87, 218
 - remove..... 183, 219
 - set 86, 217
 - show 217, 258, 261
- Disk failure.....227
- Down
 - acl241
 - identity241
- Download
 - software 177, 212
- Dummy synchronize
 - volume mirror 166, 227

E

- Enable
 - cluster failover..... 79, 185, 211
- Expand volume 158, 230
- Export
 - corrupted database 192, 213
 - problem..... 192, 213
- Expose
 - new volume243
 - volume 134, 232, 243

F

- Fabric58
- Failover..... 166, 227
 - cluster 79, 185, 211
 - disable..... 79, 185, 211
 - enable 79, 185, 211
- FC
 - connection mode.....58
 - fabric.....58

- interface show 58, 201
- node show..... 59, 202
- point-to-point 58
- port type..... 58
- private loop 58
- public loop 58
- set 58
- set speed202

File transfer

- show212

FT

- download 177, 212
- export problem213
- show212
- update.....187
- upload176
- upload software212

H

Hierarchy

- volume223

- Hot keys 19, 196

I

Identify

- storage device 85, 216

Identity

- acl add chap239
- acl add name.....239
- acl remove name239
- add srp240
- create acl238
- delete acl238
- details 128, 238
- down241
- remove chap240
- remove srp.....240
- set241
- up241

- In-band46

- Info53

- V switch200
- V-Switch171

- init.....46

- Init.....51

- V-Switch198

Initiate	
V-Switch	251
Interface	
details	203
set	178, 203
show	57, 202
show fc.....	201
Internet Storage Name Service	
.....	63, 174
Interval	
dead.....	78
keep alive	78
suspicious	78
IP	
active	73
configuration set.....	251
inactive.....	73
neighbor	73
RADIUS add	129, 242
radius remove	243
RADIUS set	242
radius show.....	131, 242
IP config	
remove.....	62, 179, 206
set	60
show	61
IP configuration	
set	178, 206
show	206
IP route	
add	67, 180, 207
config	66
default.....	67
remove.....	69, 180, 208
show	68, 207
iSCSI	
alias target.....	234
create target	234
portal create.....	233
portal remove.....	233
portal show	252
remove target	235
set target.....	235
show portal	233
show target.....	233
target details.....	117
iSCSI portal	
create.....	64
remove.....	233

show	65, 233
iSCSI target	
alias	234
create.....	234
details	117
remove	168, 235
set	167, 235
show	233
iSNS.....	63, 174

K

Keep alive interval.....	78, 211
Keep alive parameters	210
Keep alive signal	78
Key	129, 242

L

Last good configuration.....	190
LCD.....	42, 190, 250
LED	23, 35
GB indicator	31, 44
network port.....	29, 39
power indicator.....	31, 44
Load threshold.....	145
Logical Unit Number	108
LU	
details	245
remove	167, 245
show	244
LUN.....	108
carving	16, 90
details	245
remove	245
remove	167
show	244
LUNs discovery	181, 201

M

Management	41
port.....	41
Management Station	
ping from V-Switch.....	68

MIB	20
Mirror	
add	229
add volume	142
break	150, 229
dummy synchronize volume	166, 227
synchronize volume	227
volume	224
volume show	143, 227
Mirrored volume	
replace	256
Mounting	25, 36

N

N Port	58
Name	
acl identity remove	239
Neighbor	
add	76, 209
details	80, 210
remove	81, 184, 210
set	81, 184, 209
show	80, 209
Network port	29, 39
config	60
Network topology	17
New	
volume expose	243
Node	
show fc	202
Normal mode	190
Number of children	95

O

Off-line	79, 185
On-line	185
On-line copy	141
On-line replication	102, 140
Optical transceiver	39
Out-of-band	46

P

Panel	
back	34
back 2000	23
front	34
front 2000	22
Parallel SCSI bus ID	57, 204
Password	174
Ping	68
Port	
10/100	29, 40
console	30, 40, 249
copper	29, 39
FC	27, 37
fiber optic	39
management	41
network	30, 40
RJ45	29, 39
RS232	30, 40
Scalability	43
SCSI	27, 37
Telnet	171
Potential capacity	153
Power supply	186
Private Loop	58
Protocol bridging	16
PSCSI	
set	58, 204
show	57, 203
Public Loop	58

R

RADIUS	
add	129, 242
key	129, 242
remove	243
set	242
show	131, 242
Read community	55
Remove	
acl	237
acl identity chap	240
acl identity name	239
admin	199
all volume	226

all volumes.....	164
disk.....	183, 219
IP config	62
IP configuration	179, 206
IP route	69, 180, 208
iSCSI portal.....	233
iSCSI target	168, 235
lu 167	
LU.....	245
LUN.....	245
neighbor	81, 184, 210
radius.....	243
SNMP manager.....	173, 205
srp identity.....	240
storage.....	183, 219
subdisk.....	183, 221
user profile.....	175
volume	162, 226
Remove all	
volume	226
Rename	
volume	162
Replace	
mirrored volume	256
power supply.....	186
volume	165, 227
Replicate.....	262
Replicating data off-line	102,
140, 260	
Replication status.....	262
Report LUNs	181, 201
Reset.....	22, 187
V switch.....	200
V-Switch	176
Resize volume	153, 229
Retract volume	157, 230
RJ45.....	249
RS232	19, 46, 190, 249

S

Safe mode.....	190
Safe Mode	213
SCSI bus ID	57, 204
Service Agent	63
Service Location Protocol	63
Set	

acl.....	237
cluster	82, 185, 211
device.....	52, 75, 170, 182, 200
disk	86, 217
FC connection mode	58
FC port type	58
fc speed	202
FC speed	58
identity	241
interface	178, 203
IP configuration ...	60, 178, 206, 251
iSCSI target	167, 235
neighbor	81, 184, 209
p SCSI bus ID	57
RADIUS	242
SNMP manager	173, 205
srp identity.....	241
storage	86, 182, 218
subdisk	183, 221
Telnet.....	54
volume	162, 225
SFP	39
Show	
acl.....	117, 235, 237
admin	198
cluster	78, 210
disk	217
fc interface	58, 201
fc node	59, 202
file transfer	212
interface	57, 202
IP configuration	61, 206
IP route	68, 207
iSCSI portal.....	65, 233, 252
iSCSI target	233
LU	244
LUN	244
neighbor	80, 209
p SCSI	57, 203
snapshot	149
SNMP manager	204
storage	252
storage	85, 216
subdisk	91, 220
system.....	214
volume	89, 94, 221
volume mirror.....	143, 227
Simple	
volume	223
Simple volume	
create.....	93

SLP	63
Snapshot	144
show	149
SNMP	20
manager add	54, 204
manager remove	173, 205
manager set	173, 205
manager show	204
Software	
download	177, 212
update	187
upload	212
Speed	
fc set	202
set fc	202
SRP	
add identity	240
remove identity	240
Storage	
blink abort	86, 216
blink activate	85, 216
details	87, 218
discovery	216
disk set	86, 217
disk show	217
remove	183, 219
set	86, 182, 218
show	85, 216, 252
Storage is missing	219
Storage port	27, 37
configure	57
FC speed	58
SCSI bus ID	57, 204
Striped	
volume	225
Subdisk	
alias	90, 221
create	90, 219
details	91
length	90
remove	183, 221
set	183, 221
show	91, 220
Subdisks	
details	220
Suspicious interval	78, 211
Synchronize	
volume mirror ...	102, 140, 166, 227
System	

show	214
System boot	213

T

Target	
authentication	125
existing	134
new	134
Technical assistance	20
Telnet	19, 46, 50, 52, 54
set device	171, 201
Telnet port	171
Transparent	
volume	224
Trap	55

U

Up	
acl	241
identity	241
UPD port	54
Update	
software	187
Upload	
software	176, 212
User name	174
User password	174
User profile	174
add	175

V

V switch	
reset	200
V Switch	
configuration	197
V Switch configuration	197
View	
iSNS	63
snapshot	149
Volume	
add mirror	229
alias	93, 162, 223

break mirror.....	229
concatenated.....	95, 224
copy create	262
create.....	88
create activate snapshot	146
create simple.....	258, 261
details	222
expand	159, 230
expose.....	134, 232, 243
expose new	243
hierarchy	223
mirror.....	100, 224
mirror add.....	142, 229
mirror break.....	152, 229
mirror dummy synchronize.	166, 227
mirror show.....	143, 227, 262
mirror synchronize	227
mirror synchronize	102, 140, 166
number of children	95
on-line copy	142
RAID 0+1	103
RAID 10.....	103
remove.....	162, 226
remove all.....	164
rename.....	162
replace	165, 227, 258
replace mirrored	166, 226, 256
resize	156, 229
retract	157, 230
set	162, 225
show	89, 94, 221
simple	93, 223
snapshot list.....	150
snapshot show.....	149
stripe	97, 225
transparent	224

Volume configuration.....	215
---------------------------	-----

Volume create

concatenated	95, 224
mirror.....	100, 224
RAID 0+1.....	103
RAID 10.....	103
simple	223
stripe.....	97, 225
transparent	88, 224

V-Switch

configuration single IP	263
init	198
initiate.....	251
install	249
management	46
reset	176
use.....	249

V-Switch cluster

configuring	75
-------------------	----

W

World Wide Node Name	59
----------------------------	----

World Wide Port Name..	58, 201
------------------------	---------

World Wide Unique Identifier	108
------------------------------	-----

Write cache

enable	86, 217
--------------	---------

Write community	55
-----------------------	----

Write-protected	87, 218
-----------------------	---------

WWNN.....	59
-----------	----

WWPN	58, 201
------------	---------

WWUI.....	108
-----------	-----

